

Ten Post COVID Predictions
....In Page No. 6

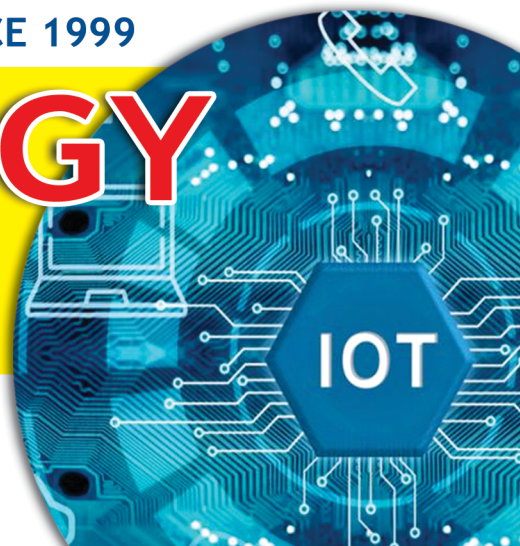
Software Testing - Careers
... In Page No. 10



THE LEADING TECH & CAREER MAGAZINE SINCE 1999

TECHNOLOGY FOR YOU

July 2020 | ₹ 20 | <https://www.technologyforyou.org>



CYBERSECURITY
UPDATES

TECH & CAREER TOPICS - INSIDE

Security & Risk Trends
COVID-19 Security Tips
Data & Privacy
IoT Real Life Applications
Laptop Tips & Tricks
Mobile Banking
AI & Key Skills
Social Media Scams
Affiliate Marketing
... and More Articles ...

Make Money with BLOG



COVID | AI | SECURITY | 5G | ANALYTICS & MORE...

THE BEST COMPUTERS & LAPTOPS CHIP LEVEL REPAIR LABS



COMPUTERS SALES & SERVICE

SPECIALISED IN REPAIRING OF

- Laptops
- All in one Systems
- CD / DVD / Blu-ray
- Projectors
- Mother Boards
- Printers / Scanners
- SMPS / UPS / Switches
- Desktops / Servers
- TFT Monitors / LCD / LED
- Hard Disk / Data Recovery



Data Recovery Experts

LAPTOPS REPAIR & RECONDITIONING EXPERTS



Google Reviews Rating

4.9/5



Justdial Rating

4.5/5



- Screen Damaged
- Hinges Broken
- Keyboard Not Working
- Cabinete/Panel Damaged
- No Power / No Display
- Mother Board Failure
- Dull Display / Junk Display
- Battery Not Charging
- Hanging while using
- Auto Restart/Power off
- Sound Not Working
- LAN/Wi-fi Not Working



114, First Floor, Chenoy Trade Centre, Park Lane,
Secunderabad-3; Ph: 040-666 26 777, 81255 26777
e-mail : sriglobalsec@gmail.com
e-mail : care.sriglobal@gmail.com
Web : www.sriglobaltechnologies.com

1-8-610, 1st Floor, Mayuri Complex
Opp : Vidyuth Bhavan (TSNPDCL), Nakkagutta,
Hanamkonda, Warangal Urban - Dist.,
Ph : 0870-2566777;
email : sriglobalwl@gmail.com

TECHNOLOGY FOR YOU

TECH | CAREERS | WEB & PRINT

The Leading Technology & Career Magazine

Estd.1999 | Vol : 21 | Issue: 7 | July 2020 | ₹ 20

PRINT & WEB EDITION | www.technologyforyou.org

FOR DIGITAL SUBSCRIPTION &

For Daily Technology,

Career & Skills

Updates visit now @

WWW.TECHNOLOGYFORYOU.ORG

Honorary Editor : C. Rama Mohana Reddy

Editor in Chief : C. Janardhan Reddy

Dy. Editor. : C. Rajasekhar

Dy. Editor : B. Sravan

Associate Editor : Hussain Shaik

Editorial Staff :

C. Dharani Kumari

C. Deepika

C. Karthika

Vamshi Mohan

Bhanu Teja

Legal Advisor : Rammohan Vedantam

Senior Manager : B.E Chandra

(Space Selling)

Marketing Executive : M.K Srinivas

Photographer : Chenna Kesava

Design & Layout: S. Yadagiri

For Advertisement Support & Subscriptions :

Cell : 98496 53985, 91822 46662

Printed, Published and owned by C. Janardhan Reddy and
Printed at Bhaskar Printers, Nallakunta, Hyd. And Published at
Vidya Nagar, O.U Road Hyderabad - 44.

Editor in Chief : C.Janardhan Reddy ; All legal matters

Subject to Hyderabad jurisdiction only.

INSIDE BYTES

Security and Risk Trends for 2020 .. 4

10 post COVID-19 predictions .. 6

11 security tips - COVID-19 .. 8

Software Testing .. 10

Data & Privacy Breaches .. 11

10 real life IoT Applications .. 12

Laptop - Fluid Damage .. 13

Mobile Banking Apps .. 14

Make Money With Blog .. 16

Top 5 Jobs in AI & Key Skills .. 18

Top Five Social Media Scams .. 20

Time to Replace Phone Battery .. 21

Skills - Digital Transformation .. 22

Six Health and Safety Factors .. 24

Affiliate Marketing .. 25

Data Analytics Careers .. 28

**MANY MORE ARTICLES INSIDE
TO IMPROVE TECH KNOWLEDGE....**

CONTACT US :

PLUS PUBLICATIONS

TECHNOLOGY FOR YOU

Mobile : 98496 53985, 91822 46662

e-mail : pluspublications@gmail.com

Website : www.technologyforyou.org

Add : #1-9-646-1/3, Adikmet Road, Beside SBI

Vidya Nagar, Hyderabad - 500 044

ONLINE ACCOUNT DETAILS

C.A.Name : PLUS PUBLICATIONS

C.A. Number : 060411100001653

IFSC Code : ANDB0000604

Bank Name & Branch : Andhra Bank,
Vidyanagar, Hyderabad

FOR DAILY TECH & CAREER UPDATES VISIT @ www.technologyforyou.org



Gartner Top 9 Security and Risk Trends for 2020

CISOs should understand these trends to practice strong planning and execution of security initiatives.

The shortage of technical security staff, the rapid migration to cloud computing, regulatory compliance requirements and the unrelenting evolution of threats continue to be the most significant ongoing major security challenges. However, responding to COVID-19 remains the biggest challenge for most security organizations in 2020.

"The pandemic, and its resulting changes to the business world, accelerated digitalization of business processes, endpoint mobility and the expansion of cloud computing in most organizations, revealing legacy thinking and technologies," says Peter Firstbrook, VP Analyst, Gartner.

COVID-19 refocused security teams on the value of cloud-delivered security and operational tools that don't require a LAN connection to function, reviewing remote access policies and tools, migration to cloud data centers and SaaS applications, and securing new digitization efforts to minimize person-to-person interactions.

Gartner has identified nine annual top trends that are the response by leading organizations to these longer-term external trends. These top trends highlight strategic shifts in the security ecosystem that aren't yet widely recognized but are

expected to have broad industry impact and significant potential for disruption.

Trend No. 1: Extended detection and response capabilities emerge to improve accuracy and productivity

Extended detection and response (XDR) solutions are emerging that automatically collect and correlate data from multiple security products to improve threat detection and provide an incident response capability. For example, an attack that caused alerts on email, endpoint and network can be combined into a single incident. The primary goals of an XDR solution are to increase detection accuracy and improve security operations efficiency and productivity.

"Centralization and normalization of data also helps improve detection by combining softer signals from more components to detect events that might otherwise be ignored," says Firstbrook.

Trend No. 2: Security process automation emerges to eliminate repetitive tasks

The shortage of skilled security practitioners and the availability of automation within security tools have driven the use of more security process automation. This technology automates computer-centric security operations tasks based on predefined rules and templates.

Automated security tasks can be performed much faster, in a scalable way

and with fewer errors. However, there are diminishing returns to building and maintaining automation. SRM leaders must invest in automation projects that help to eliminate repetitive tasks that consume a lot of time, leaving more time to focus on more critical security functions.

Trend No. 3: AI creates new security responsibilities for protecting digital business initiatives

AI, and especially machine learning (ML), continues to automate and augment human decision making across a broad set of use cases in security and digital business. However, these technologies require security expertise to address three key challenges: Protect AI-powered digital business systems, leverage AI with packaged security products to enhance security defense and anticipate nefarious use of AI by attackers.

Trend No. 4: Enterprise-level chief security officers (CSOs) emerge to bring together multiple security-oriented silos

In 2019, incidents, threats and vulnerability disclosures outside of traditional enterprise IT systems increased and pushed leading organizations to rethink security across the cyber and physical worlds. Emerging threats such as ransomware attacks on business processes, potential siegeware attacks on building management systems, GPS spoofing and continuing OT/IOT system vulnerabilities straddle the cyber-

physical world. Organizations primarily focused on information-security-centric efforts are not equipped to deal with the effect of security failures on physical safety.

As a result, leading organizations that deploy cyber-physical systems are implementing enterprise-level CSOs to bring together multiple security-oriented silos both for defensive purposes and, in some cases, to be a business enabler. The CSO can aggregate IT security, OT security, physical security, supply chain security, product management security, and health, safety and environmental programs into a centralized organization and governance model.

Trend No 5. Privacy is becoming a discipline of its own

No longer “just a part of” compliance, legal or auditing, privacy is becoming an increasingly influential, defined discipline of its own, affecting almost all aspects of an organization.

As a rapidly growing stand-alone discipline, privacy needs to be more integrated throughout the organization. Specifically, the privacy discipline co-directs the corporate strategy, and as such needs to closely align with security, IT/OT/IoT, procurement, HR, legal, governance and more.

Trend No. 6: New “digital trust and safety” teams focus on maintaining the integrity of all interactions where consumer meets the brand

Consumers interact with brands through an increasing variety of touchpoints, from social media to retail. How secure the consumer feels within that touchpoint is a business differentiator. Security for these

Artificial Intelligence, and especially machine learning (ML), continues to automate and augment human decision making across a broad set of use cases in security and digital business. However, these technologies require security expertise to address three key challenges: Protect AI-powered digital business systems, leverage AI with packaged security products to enhance security defense and anticipate nefarious use of AI by attackers.

touchpoints is often managed by discrete groups, with specific business units focusing on areas they run. However, companies are increasingly moving toward cross-functional trust and safety teams to oversee all the interactions, ensuring a standard level of safety across each space where consumers interact with the business.

Trend No. 7: Network security transforms from the focus on LAN-based appliance models to SASE

Cloud-delivered security services are growing increasingly popular with the evolution of remote office technology. Secure access service edge (SASE) technology allows organizations to better protect mobile workers and cloud applications by routing traffic through a cloud-based security stack, versus backhauling the traffic so it flows through a physical security system in a data center.

Trend No. 8: A full life cycle approach for the protection of the dynamic requirements of cloud-native applications

Many organizations use the same security product on end-user-facing endpoints as they did for server workloads, a technique that often continued on during “lift and shift” cloud migrations. But cloud-native applications require different rules and techniques, leading to the development of cloud workload protection (CWPP). But as the applications grow increasingly dynamic, the security options need to shift as well. Combining CWPP with the emerging cloud security posture management (CSPM) accounts for all evolution in security needs.

Trend No. 9: zero-trust network access technology begins to replace VPNs

The COVID pandemic has highlighted many of the problems with traditional VPNs. Emerging zero-trust network access (ZTNA) enables enterprises to control remote access to specific applications. This is a more secure option, as it “hides” applications from the internet — ZTNA only communicates to the ZTNA service provider, and can only be accessed via the ZTNA provider’s cloud service.

This reduces the risk of an attacker piggybacking on the VPN connection to attack other applications. Full-scale ZTNA adoption does require enterprises to have an accurate mapping of which users need access to what applications, which will slow adoption.

Data Analytics



Data analysis is a process of inspecting, cleansing, transforming, and modeling data with the goal of discovering useful information, informing conclusions, and supporting decision-making. Data analysis has multiple facets and approaches, encompassing diverse techniques under a variety of names, while being used in different business, science, and social science domains. In today's business, data analysis is playing a role in making decisions more scientific and helping the business achieve effective operation.

Data mining is a particular data analysis technique that focuses on modeling and knowledge discovery for predictive rather than purely descriptive purposes, while business intelligence covers data analysis that relies heavily on aggregation, focusing mainly on business information. In statistical applications, data analysis can be divided into descriptive statistics, exploratory data analysis (EDA), and confirmatory data analysis (CDA). EDA focuses on discovering new features in the data while CDA focuses on confirming or falsifying existing hypotheses. Predictive analytics focuses on application of statistical models for predictive forecasting or classification, while text analytics applies statistical, linguistic, and structural techniques to extract and classify information from textual sources, a species of unstructured data. All of the above are varieties of data analysis.

KPMG Law's Top 10 post COVID-19 predictions

As the Australian and global economies move from the COVID-19 crisis into a 'New Reality' phase, a 'BUILD BACK BETTER' approach will be essential according to Stuart Fuller, Global Head of Legal Services, KPMG.

That will be about retaining and leveraging the lessons learned from COVID, but it will also be about developing better more flexible ways of working – and the greater use of technology and automation. As Global Head of Legal Services at KPMG International, Stuart Fuller has a broad lens on the key issues that will play out in business in the coming 12 months.

"The COVID-19 'Reaction Phase' required commercial, operational and regulatory resilience," said Mr Fuller. "Business was thrust into what we call the 'Resilience Early Recovery Phase' with active contract and counterparty management and a flexible approach reflecting the exercise of caution. Whilst this phase enabled some fast capital raises, it also saw slower deal execution and a high level of 'Business As Usual' disruption. Yet we've also seen employment arrangements in transition and which will be reshaped for the longer term; at the same time, there's been a strong move to the world of virtual governance and stakeholder engagement."

Mr Fuller says that while the short term focus will be on the need to 'fix the issues' from the COVID-19 period, businesses will have to manage big decisions made at speed in imperfect conditions.

"That's where they must plan and implement resilience measures and mechanisms in three key areas, and appreciate that the business needs legal, and the legal is business," he says. "We're already seeing the early movers starting to consider these three: supply chain resilience, business reorganization, and the regulatory engagement/response highlighting the role of Legal."

KPMG Law makes Ten Post COVID-19 Predictions that can guide business as they look to respond to a faster more digitised way of operating and 'Build Back Better'.

Top ten post COVID-19 predictions for business

1. Business will shift focus to the 'Client Experience' – Solutions, services and the client experience will TRIUMPH over advice, expertise and legacy relationships.
2. Collaboration' will reshape the market – Market dynamics and demand will be elastic and will drive a new era of what KPMG Law calls 'COLLABORTITION' – the place where Collaboration and Competition meet.
3. We will automate – the legal marketplace will augment its services delivery through automation. That's already underway but it will intensify as businesses seek to further simplify, modernise, and digitise to drive a better customer experience and revenue for the business.
4. We will see intensification of digitisation – What might have taken a decade, will now be intensified by rapid digitisation in a shorter time frame. In the legal world, all

areas will be impacted from law schools and law firms to limbs of government and court systems.

5. Legal sovereignty will follow economic sovereignty – And it will impact foreign investment – especially in Asia – trade, and immigration trends.

6. Resilience will trump efficiency – In a more complex and competitive world, legal will be the enhanced enabler, the "muscle" and "connective tissue" of business and which will help business bake in and embed resilience.

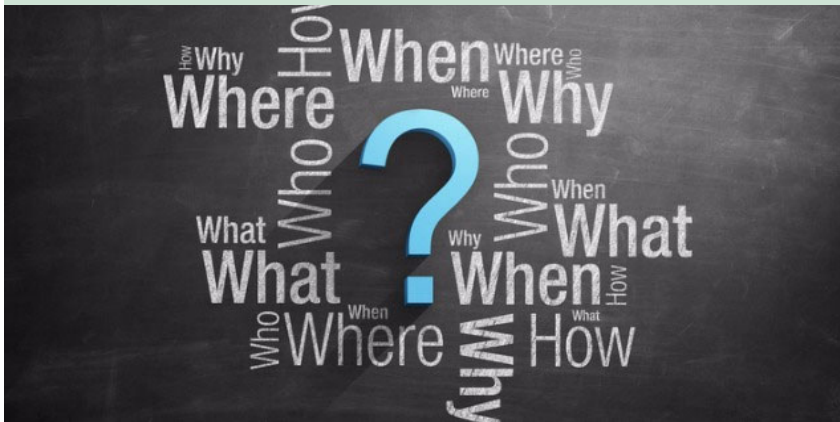
7. Business will need the benefit of hindsight – Looking back at preparedness and strategy will be a powerful weapon for shaping both corporate strategy – and managing the inevitable claims that will flow from COVID.

8. They will be back but not as we know them – Both governance and compliance will return to the spotlight for business, but will not be the same as before.

9. There will be greater expectations – Regulatory, political and community expectations will continue to increase leading to more demands on business and legal.

10. We will see embedded legal eagles – The role and value of legal will be redefined in an organisation with a much more embedded character and crucial role to play in the business; ie business will recognise it needs legal; and legal is business.

3 Reasons Why Curiosity Is Essential For The Future - And You Should Care



by Enrique Rubio - Tech and HR Evangelist

✍️ Let's start by running a little experiment

Ask yourself any question : why is the sky blue? what are those shiny things in the night sky? Why do you get allergies in the Spring?

Google your question.

How many results did you get? – Probably millions.

If you ask the questions that others have asked before, you will most likely get the answers that already exist. And if those questions and answers are already available, then they can be fed into an artificial intelligence computer as a big pile of data.

It will be extremely difficult for humanity to make a difference in the future of work and life just by memorizing facts, ideas or pre-existing questions and answers. When it comes to storing existing data and information, we don't stand the slightest chance to compete with technology.

So, the question becomes : how are we going to differentiate ourselves from intelligent machines?

Most futurist people and organizations agree that it is by being increasingly better at the things that are uniquely human: collaboration, critical thinking, creativity and imagination, emotional intelligence, empathy, among others.

But I think we need more. There's got to be something else.

And I am fairly convinced that the most fundamental differentiator between humanity and the herds of robots that will be coming to work and live with us is this: curiosity.

Curiosity isn't a trait unique to humans. Cats and dogs are curious too, and many other earthlings in beautiful planet Earth. But we have excelled at being curious over any

other species that have existed. It's because our curiosity that we have been able to make the greatest discoveries, innovations and progress. "Why is the sky blue"? asked someone once, and science was created as a result.

The greatest innovators and scientists in our history have been, over any other thing, the most curious people you could find. Yes, they were incredibly smart. But they draw their inspiration, ideas and, perhaps, their intelligence, from the reservoir of their insatiable curiosity and the questions they asked. Even Albert Einstein said "I have no special talent, I am passionately curious".

» Why Is Curiosity Important?

1. Curiosity allows us to unveil new knowledge

Every single innovation and discovery started with a question. Being curious and asking questions is the most powerful way to unveil new knowledge and ideas. You can't start with a hypothesis about something that you haven't asked yourself before. When you are curious about things and people, you have the opportunity to see something that might be invisible to others. And maybe that "something" becomes the next greatest innovation, discovery, company or solution.

2. Curiosity is a key differentiator

We are in the era of artificial intelligence. It is absolutely impossible for us to compete with machines in the things that they are good at: processing data, connecting existing information, memorizing facts and data, processing transactional, step-by-step, repetitive activities. They are and will always be better than us at those things. But ultimately, machines aren't capable to envision things and ask themselves questions that haven't been fed to them. No technology or animals have that

capability, and humans do! Don't try to compete with technology in the things technology is good at. Make yourself more valuable and relevant by being extremely curious, even about mundane things. That's the key differentiator.

3. Curiosity helps us add new value

How do we measure the amount and quality of the value we add at work? You could say: by how hard you work, by how much you deliver, by the cost-benefit of the ideas you implement, or the ROI or the project you do. I'd say: all that is true. But, right now, the business and professional landscapes are getting much more competitive. More companies and startups are popping up everywhere and more people will be trying to access jobs. A lot of them will compete by trying to squeeze more value out of things that already exist. And my approach to that would be: how do we create new value? Where do we find that new value? In the only place where it exists: in the unknown! Yes, we don't know! And because we don't know, we must ask ourselves questions, over and over again. By being curious we could find areas that have escaped from everybody's sight before. In doing so, we can find areas where we can new value altogether!

» Why Should You Care

About Curiosity?

We are entering a very "weird" stage in human cultural and mental evolution. We are living in exciting, fascinating, transformative, yet difficult, competitive and complex times.

As technology continues its relentless and exponential forward motion, more and more is going to be demanded from us, humans, both in our personal and professional lives. We are going to be required to create, add and deliver much more value than ever before. If we don't, we could be equally dead.

It's fundamental for us to understand that technology will be taking over millions of roles that we have historically occupied at work and life. Machines will be very relevant in the future, more productive, efficient, fast and competitive than we can ever dream to be. But they will be so in areas that were already performed mediocrly by humans. For example, we don't have much physical strengths, machines do. We can't store too much data, machines can. Why would we try to outcompete machines in that?

Instead, let's be much better, way, way, way better, at what we were naturally gifted with: our capacity to envision and imagine wonderful things and making them happen, beginning by being radically curious.

Ask questions. Observe the world. Be curious.

11 security tips to help stay safe in the COVID-19 era

By Keshav Dhakad, Group Head & Assistant General Counsel Corporate, External & Legal Affairs, Microsoft India.

The COVID-19 pandemic has changed our daily routines, the ways we work, and our reliance on technology. Many of us are now working remotely, students are attending classes virtually, and we're relying more on social media and social networks to stay connected as we define what our new normal looks like.

As we spend more time online, it's important to remember that the basics of online safety have not changed. These guidelines provide a strong foundation for digital security, but as we think about the "new normal" and how the internet is woven into the fabric of our lives, extra steps may be necessary to further reduce risk.

So, in addition to the security policies implemented by your work or school, here are a few more practices we recommend you—and your family and friends—adopt to further increase personal cybersecurity resilience.

Keep devices secure and up to date

Turn on automatic security updates, antivirus, and firewall. The reality of cyber threats is that they often prey upon the devices that are the easiest to compromise: those without a firewall, without an antivirus service, or without the latest security updates. To reduce this risk, turn on automatic updates to ensure your devices have the latest

security fixes, enable or install an antivirus solution that runs continuously, and configure a firewall. Modern computers have many of these features available and enabled by default, but it is a good idea to check all three are correctly set up.

Don't forget networking devices. Device safety includes your networking devices, too. As with computing devices, make sure that you check for and apply all updates for your networking devices. Many devices use default passwords, which means attackers have an easy list to try. Make sure to check your networking devices are not using default admin passwords or ones that are easily guessable (like your birthday). It's also good hygiene to update your Wi-Fi credentials to strong passwords with a mix of upper- and lowercase letters as well as symbols and numbers.

Use Wi-Fi encryption options for access. Wireless access points offer the ability to require passwords to gain access to the network. You should take advantage of this feature to ensure only authorized users are on your home network.

Secure your identity, guard your privacy

Protect your digital identity. With more of our lives connected in the virtual realm, your digital identity becomes even more important to protect. Use strong passwords or, if possible, biometric authentication like your face or fingerprint, and wherever possible enable multi-factor authentication (MFA). Among others, Google and Microsoft

both offer free MFA applications that are easy to set up and use.

Keep your guard up in online chats and conferencing services. As we spend more time on virtual conferences and video calls, it is important to think about privacy. Consider these questions when trying new services:

Who can access or join the meeting/call?

Can it be recorded? If yes, do all participants know?

Are chats preserved and shared?

If there is file sharing, where are those files stored?

Use background blur or images to obscure your location. One of the more popular features on video conferencing tools like Zoom, Skype, and Microsoft Teams is the ability to blur or change your background. This can be an important privacy step that you can take to maintain privacy between home and work environments.

Protect business data while at home

Use the right file-sharing service for the right task. While working remotely, it's easy for lines to blur between work and home. It's important to ensure that your business data does not get mixed with your personal data. Remember to use business resources, like SharePoint or OneDrive for Business, to store and share content for work. Don't use consumer offerings for business data while you are remote. Where possible, consider enabling Windows Information



Protection to reduce the risk of unintentional (and intentional) enterprise data leakage via consumer services.

Turn on-device encryption. Device encryption ensures that data on your device is safe from unauthorized access should your device be stolen or lost.

Be aware of phishing and identity scams

Cybercriminals continue to exploit victims even through this global crisis. Based on what Microsoft has observed over the last two months, cybercriminals are utilizing new lures related to the coronavirus outbreak and are being indiscriminate in their targeting. As we move into this "new normal" of more virtual engagement, the same vigilance you kept at the office or classroom applies at home.


Here are a couple of observed attack methods to keep top of mind:

Identity compromise is still the number one point of entry. Attackers are looking to steal your digital identity for monetization, spam, and access. Be on the lookout for unexpected websites and applications asking you to sign in with your credentials. The same goes for MFA requests. If you did not initiate the request, do not verify it. Report suspected sites and uninitiated authentication requests through your browser or applications.

Phishing is still out there. Be wary of offers that are too good to be true, pressure time, or promise a free prize. These are the same bad guys from before, but now they're using the outbreak and public fear to drive a different action. For more information on phishing attacks, read Protecting against coronavirus themed phishing attacks.

Don't fall victim to tech support scams. Tech support scams are an industry-wide issue where scammers use scare tactics to try and trick you into paying for unnecessary services that supposedly fix a device, operating system, or software problem. Please note that Microsoft will never contact you with an unsolicited offer to address a technical issue. And error and warning messages in Microsoft products never include a phone number to call. If you receive an unsolicited tech support call telling you there is something wrong with your computer even if the caller offers to correct the issue for free hang up and report the call to <https://www.microsoft.com/reportascam>.

Be Safe While Being Social Online

 The advent of the internet has brought the world closer and made it possible for you to interact with your social circles right from your mobile device or PC. Moreover, social media platforms like Facebook, Twitter etc. have made it easier than ever to keep the people who matter to you updated about the happening in your life. It is no wonder then, that almost everyone has a presence on these platforms. But while this is the positive side of the online social world, there is also another more negative side to all of this.

A recent survey by Cybersecurity firm Norton by Symantec conducted in 2017 shows that online harassment is increasing in India, with 80% of the surveyed users admitting to have encountered some form of it. Online harassment can manifest in many forms. We've listed some of the most common ways in which you can be harassed online and also some ways in which you can protect yourself against these risks:

Identity Theft ...

If you're on Social Media, chances are that you have personal information - like your photographs, details of your educational background, your relationships - floating around. This gives online fraudsters the opportunity to take this information and use it to commit frauds or unlawful acts. For example, fraudsters obtain private details like your Aadhaar card number or personal information like email ID and then uses it to carry out fraudulent or illegal activities, landing you in trouble. Sounds scary? It is.

Cyber Stalking ...

Have you ever taken a look at the Message Requests you get in your 'Other Folder' on Facebook? If yes, and especially if you're a woman, you would have definitely received disturbing messages from strangers. This is just a very basic level of cyberstalking and has been known to escalate very easily. Not just strangers, but there is an increasing number of cases of cyberstalking by acquaintances, friends, and family as well. Not only can this be very frustrating and annoying, but can also lead to a situation where it becomes menacing and terrifying. And it can easily happen to anyone.

Media Liability ... Most of us consider our Social Profiles the place from where we can express our opinions. But what happens when someone takes something you posted, takes it out of context and misrepresents your point of view? It sounds harmless, but it can land you in serious legal trouble. For example, if you create a podcast/blogs and someone hacks into it, takes control of it and puts out content that is defamatory, infringes on any intellectual property or results in an invasion of an individual's rights of privacy then you can land in legal trouble.

So how do you protect yourself...?

Some basic practices you can follow to prevent such situations are :

- » Set strong passwords and don't share them with anyone.
- » Check the privacy settings of your social profile and make sure that you've enabled the setting that prevents unconnected people from viewing your details or downloading your images
- » Never share sensitive details like your phone number, address or email address on your social profile, and if you do, make sure that they are hidden from the public
- » Don't engage with strangers, no matter how familiar they seem.
- » Censor yourself while posting via your social profiles.
- » Accept requests only from known users.
- » While these measures will keep you protected to some extent, anti-social elements that want to cause harm will always find a way to do so. In case you find yourself in an uncomfortable situation online, you should report the incident or the user who is causing trouble for you. You can also lodge a complaint with the Cyber Cell in case things get out of hand. Our Individual Cyber Safe Insurance will ensure that the financial setbacks that you could incur due to such an event get minimized.

Software Testing - A Career Option For Fresh Aspirants



✍ The ambition to become a software tester is common and is worth praising because of the fast-growing significance and cost-effectiveness of the job. With software testing name, it refers to a procedure that is conducted to ensure the quality and standard of a product or service. This analyzing procedure matters significantly additionally, as it helps to understand the potential risks involved in the implementation of software. The test helps in jumping to the conclusion that the software is designed and developed to comply with the technical needs of a product/service.

The Significance of Software Testing Careers Today

As a college graduate who has earned his/her graduate degree, maybe you are in a state of confusion to resolve which career stream to pursue? If you guess you give scrupulous attention to details and are interested in pursuing a sedentary job that can help you maximize your precision and have a tendency towards software development then pursuing software testing careers in India is worth the idea. Another very important reason to choose a software testing job is because it is growing rapidly and has a panoptic scope. With that said, it is understandable that there will be a requirement of more and more personnel on a regular basis and therefore numerous job opportunities are plentiful in the industry.

The IT industry has produced a sensation in India and the establishment of various well-known IT parks in cities such as Pune, Bangalore, Hyderabad, Mumbai, Chennai,

Noida, etc. has opened several job opportunities for the aspirants. With that said, there is no lack of testing jobs in India for the accomplished professionals, intermediate as well as beginners to choose testing job as a highly cost-effective career choice. Because a maximum number of industries have hi-tech functions, software programs are developed to fit a variety of industry needs. However, as a matter of fact, it is not likely for every organization to deal with its private software production or testing units. Therefore, such QA service providers have evolved as an independent entity offering testing as a standalone service.

Benefiting of launching your career in software testing :

- ▶ Considering the rapidly growing significance and demand for software universally, it is affordable to guess that the demand for the prolific software testers will never wither.
- ▶ Software testing has a clear-cut career path.
- ▶ It transmits transferable skills as well as a second-to-none grounding/knowledge base for other career fields
- ▶ Since no projects are identical, so there is some diversity in the workload.
- ▶ The industry has certifications, so you can leverage to move your career up.

What can you get out of software testing jobs?

For every development process, the role of QA matters fundamentally, as it is very instrumental in evaluating quality and

documents that contribute to augment service level. Jobs in this industry require high levels of accuracy and profound knowledge of the field. With the help of software testing end to end, a professional is able to discover errors and bugs which can later easily be dealt with before the software is delivered.

India is one of the well-known hubs of the IT industry and the demand for software and IT services are invariably shooting up. With that said, there will always be a need for testers for carrying out testing. It is easy to understand that those looking to set up software testing careers can have a very bright and hopeful future; they can look forward to a lucrative career which can go on to build a strong base for a satisfying career.

Conclusion ... The software testing industry offers a vast and mushrooming demand for its services, clear-cut career paths, and the competence to learn transmittable skills, and therefore offers second-to-none career opportunities for go-ahead individuals.

While a career in software testing is hopeful and cost-effective, it is not a right thing for every aspirant. If you are indeed not highly interested, lack the skills, or if getting into strategic details hassle you, then software testing is not suitable for you. However, if you are methodical, delight in solving problems, and have the right skills, then career in software testing is the ticket for you. You can join a software testing training in Bhopal to nurture your skills in this IT field and look forward to a very hopeful future.

Best Practices to Prevent Data & Privacy Breaches



✍ Before we get started, let's define what we're talking about. The term security breach can conjure up all sorts of meanings, but I'd like to focus on how it relates to information technology. So by definition ...

» **Security breach** : A situation where an individual intentionally exceeds or misuses network, system, or data access in a manner that negatively affects the security of the organization's data, systems, or operations.

When it comes to data breaches, the risk for organizations is high, from the easily calculable costs of notification and business loss to the less tangible effects on a company's brand and customer loyalty.

Let's look at some ways that will significantly increase the effort required to breach the security of your network and computers.

» Change Default Passwords

It's surprising how many devices and applications are protected by default usernames and passwords. Attackers are also well aware of this phenomenon. Not convinced? Run a Web search for default passwords, and you will see why they need to be changed. Using good password policy is the best way to go; but any character string other than the default offering is a huge step in the right direction.

» Never Reuse Passwords

On more than one occasion, you must have run into situations where the same username/password combination was used over and over realizing it's easier. But if you know this, I'm pretty sure the bad guys do as well. If they get their hands on a username/password combination, they're going to try it elsewhere. Don't make it that easy for them.

» Look Beyond IT Security While Assessing Your Company's Data Breach Risks.

To eliminate threats throughout the organization, security must reach beyond the IT department. A company must evaluate employee exit strategies (HR), remote project protocol, on- and off-site data storage practices, and more-then establish and enforce new policies and procedures and physical safeguards appropriate to the findings.

» Establish A Comprehensive Data Loss Protection Plan

Your efforts will demonstrate to consumers and regulators that your organization has taken anticipatory steps to address data security threats. Disseminate this plan throughout the management structure to ensure everyone knows what to do in the event of a breach.

» Examine Security Logs

Good administrators know about baselining and try to review system logs on a daily basis. Since this article deals with security breaches, I'd like to place special emphasis on security logs, as they're the first line of defense.

» Do Regular Network Scans

Comparing regular network scans to an operational baseline inventory is invaluable. It allows the administrator to know at a glance if and when any rogue equipment has been installed on the network.

One method of scanning the network is to use the built-in Microsoft command net view. Another option is to use freeware programs like NetView. They're typically in a GUI format and tend to be more informative.

» Provide Training and Technical Support to Mobile Workers.

Ensure that the same standards for data security are applied regardless of location, by providing mobile workers with straightforward policies and procedures, ensuring security and authentication software is installed on mobile devices and kept up-to-date, and providing adequate training and technical support for mobile workers.

» Keep Security Software Updated (Or Patches).

An unpatched system is, by definition, operating with a weak spot just waiting to be exploited by hackers. Admittedly, applying patches takes time and resources, so senior management must provide guidance on allocations and expectations.

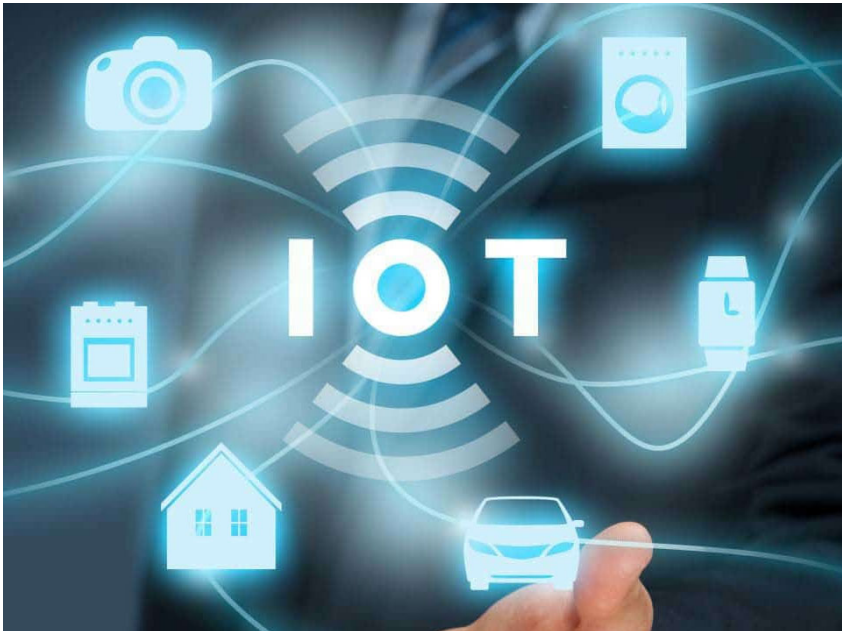
» Don't Rely On Encryption as Your Only Method of Defense.

Encrypting data in transit and at rest is a best practice, but, when used alone, it can give businesses a false sense of security. Although the majority of state statutes require notification only if a breach compromises unencrypted personal information, professionals can and do break encryption codes.


» **Monitor Outbound Network Traffic** .. Malware is becoming sophisticated enough to avoid detection. One method of exposing it is monitoring outbound network traffic. Suspicious should be raised when the number of outbound connections or the amount of traffic deviates from normal baseline operation. To tell the truth, it may be the only indication that sensitive information is being stolen or that an email engine is actively spamming.

These methods are simple to implement and will surely go a long way toward making it more difficult for a security breach to occur.

10 real life Applications of IoT that are so cool..!



by Naveen Joshi
Founder & CEO - Allerin, Mumbai

 The power of internet connectivity has now stepped beyond computers and smartphones. Every 'smart' device around us is now aiming to solve real world problems with digital interventions. **These are the real life applications of IoT (Internet of Things).**

Needless to mention, the buzz around IoT is immense. This disruptive technology is penetrating into various industries, developing new real-life applications of IoT and connecting every internet-enabled device around us. According to one survey, it is expected that there will be 31 billion connected devices by 2020. But amongst the mad rush of 'newer' and 'better' IoT applications, some shine through more than the rest. Here's our list of the coolest ones that blew our minds!

» Smart toothbrush

A smart toothbrush is embedded with high-quality sensors that capture data on your brushing frequency, missed spots, the pressure applied, and so on. You can track all of this crucial information on your smartphone and gain insights on how to improve your oral health.

» Fitness Trackers

Are you a fitness freak? Now, IoT-connected devices are here to help you

stay fit. Fitness trackers help you track your daily activities such as your sleeping patterns, your heart rate, activity patterns, workout statistics, calories burned, and so on. Armed with this information, you can monitor and plan your fitness goals easily.

» Child and Pet finder

The feeling of losing your loved ones, be it your kid or a four-legged member of your family, is terrifying. But, with an IoT-connected device that is connected to your smartphone, you can track their location in real-time. Thus, IoT enables you to stay in peace even when you are away from your loved ones.

» Infant monitor

There is good news for all the new parents out there! You can monitor your baby's daily activities on your smartphone in real-time from anywhere in the world. Infant monitors give you information on your baby's respiration statistics, sleeping positions, sleeping duration, body temperature, and so on.

» Smart shelves

With sensors, cameras, and actuators embedded on shelves, retailers can get real-time updates on products, enabling them to replenish when needed. IoT also helps retailers get real-time alerts of misplaced products on their smart devices.

» Smart gardening

No free time to water your plants? You can try smart gardening, instead. With sensors embedded in your garden, you can get information on the condition of the soil, temperature, humidity level, and suggestions for the right time to watering plants. All of these data points can be easily controlled and managed on your smartphone.

» Health monitoring

Getting periodic information about the status of your kids' or old parents' health has become an essential requirement these days. Now, health-tracking devices help you to monitor their health in real-time. Sudden changes in temperature, blood pressure, heart rate, breathing, etc. are notified to you, thereby allowing you to take necessary actions on time.

» Smart refrigerator

How cool it is to peek into your fridge without opening its door! This thought is no more a fantasy now! The sensors and cameras attached to new-age smart refrigerators allow you monitor spoiled food items. Additionally, it enables you to track leftover food without opening its door.

» Pollution warnings

Smart air monitors detect pollutants emitted from vehicles in a particular region, affecting the environment. Such real-time updates to government agencies help them take required steps quickly.

» Smart shoes


Smart shoes allow users to change the color of the shoe with one tap on their smartphone! With the tap of your heels, you can also send a text message to your friends, call a cab, monitor your steps, calories burned, and so on.

Honestly, we are already enjoying applications that we never thought of, a few years back. As the concerns around robust network connectivity, security, and privacy get resolved, we will see more groundbreaking applications disrupting our lives.

"The IoT (Internet of Things) is being called the fourth Industrial revolution and is expected to have a value of over \$ 10 trillion by 2025".

- McKinsey Global Institute

How To Protect A Laptop From Fluid Damage

 This article teaches you how to prevent your laptop from sustaining damage immediately after spilling a liquid on it. Keep in mind that although the following information is the best way to handle a spill yourself, there is no guarantee that your laptop will be stored safely; similarly, seeking professional help is a far better solution.

Short Summary :

- » Unplug the laptop and turn it off.
- » Take the laptop out of the liquid.
- » Turn the laptop over and remove the battery.
- » Disconnect the external equipment.
- » Open the laptop and place it on a towel.
- » Wipe off any remaining liquid.
- » Remove all the material you can.
- » Dry internal components and remove any residue.
- » Allow drying for at least 24 hours before turning it on.

Steps :

1. Turn off the laptop and disconnect it from its power source immediately

To do so, just hold down the laptop's power button. If the liquid touches the circuits on the laptop while they are active, your laptop will most likely shorten, so the time is very important.

To disconnect the laptop from a power source, simply remove the charging cable from the laptop. It is usually on the left or right side of the laptop.

2. Remove the laptop from the residual liquid ...

This will both minimize your laptop's exposure to more liquid and decrease the risk of electrical shock.

3. Turn the laptop upside down and remove the battery if possible ...

You can usually do this by flipping your laptop over, sliding a panel from the bottom of the laptop and gently pulling on the battery.

This step is not possible on a MacBook without first unscrewing the bottom of the laptop from the rest of the housing.

4. Unplug all external hardware ...

This includes the following items:

USB devices (flash drives, wireless adapters, chargers, etc.)

Memory cards

Controllers (e.g., your mouse)

The laptop charger

5. Place a towel on a flat surface ...

Here, you will configure your laptop for the next few days, so choose a hot, dry and unobtrusive area.

6. Open your laptop as much as possible and place it on the briefcase

Depending on the flexibility of your laptop, everything from a laptop under the tent to a completely flat laptop will be possible. To speed up the process of drying the liquid, you can get a quick fix on the liquid to help.

7. Wipe all visible liquids ...

To clean are the front and back of the screen, the case of the laptop and the keyboard.

Make sure your laptop is always with you while you do this.

8. Ground yourself before touching the internal components of your computer

Grounding eliminates static electricity from your clothes or your body. Static electricity can easily destroy the circuit, so it is important to do this step before touching the RAM card or hard drive.

9. Remove all the material you can...

If you are not familiar with removing RAM,

your computer's hard drive, and other internal removable components, you should bring your laptop to a professional repair service instead.

You can not find anything else for your specific material. Just search the factory and model number of your computer followed by "RAM Removal" (or the component you want to delete).

For a MacBook, you are one of the most successful builders in the world.

10. Dry all wet internal components...

To do this, you will need a microfiber cloth (or other lint-free cloth).

If there is too much water in your laptop, you must first empty it. Be extremely sweet.

11. Remove dry residues ... Use a lint-free cloth to gently remove all non-water stains, chippings, and other non-liquid residues.

12. Let your laptop dry... You'll want to leave it alone for at least one day.

Remember to store your laptop in a dry, warm place. For example, a dehumidifier can improve the drying time.

Never use a hair dryer to speed up the drying process of your laptop because the heat concentration of a hair dryer is strong enough to damage the internal parts of your laptop.

13. Reassemble the laptop and turn it on...

If it does not start or if you notice a distortion in the sound or the display, you must entrust your laptop to a professional laptop repair service (for example, a Best Buy technical service).

14. Remove all residues if necessary

Even if your laptop is up and running, you may have to deal with a sticky or oily substance. You can remove this debris by gently rubbing the affected area with a damp, lint-free cloth as you did when the laptop was drying.

Increased use of Mobile Banking Apps could lead to Exploitation



As the public increases its use of mobile banking apps, partially due to increased time at home, the FBI anticipates cyber actors will exploit these platforms.

Americans are increasingly using their mobile devices to conduct banking activities such as cashing checks and transferring funds. US financial technology providers estimate more than 75 percent of Americans used mobile banking in some form in 2019.

Studies of US financial data indicate a 50 percent surge in mobile banking since the beginning of 2020. Additionally, studies indicate 36 percent of Americans plan to use mobile tools to conduct banking activities, and 20 percent plan to visit branch locations less often. With city, state, and local governments urging or mandating social distancing, Americans have become more willing to use mobile banking as an alternative to physically visiting branch locations. The FBI expects cyber actors to attempt to exploit new mobile banking customers using a variety of techniques, including app-based banking trojans and fake banking apps.

App-Based Banking Trojans

The FBI advises the public to be cautious when downloading apps on smartphones and tablets, as some could be concealing malicious intent. Cyber actors target banking information using banking trojans, which are malicious programs that disguise themselves as other apps, such as games or tools. When the user launches a legitimate banking app, it

triggers the previously downloaded trojan that has been lying dormant on their device. The trojan creates a false version of the bank's login page and overlays it on top of the legitimate app. Once the user enters their credentials into the false login page, the trojan passes the user to the real banking app login page so they do not realize they have been compromised.

Fake Banking Apps

Actors also create fraudulent apps designed to impersonate the real apps of major financial institutions, with the intent of tricking users into entering their login credentials. These apps provide an error message after the attempted login and will use smartphone permission requests to obtain and bypass security codes texted to users. US security research organizations report that in 2018, nearly 65,000 fake apps were detected on major app stores, making this one of the fastest-growing sectors of smartphone-based fraud.

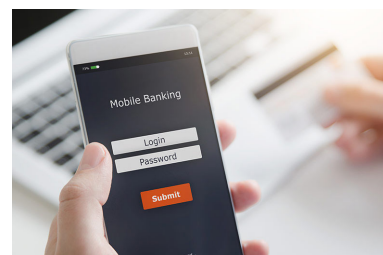
TIPS TO PROTECT YOU AND YOUR ORGANIZATION

Obtain Apps from Trusted Sources

Private sector companies manage app stores for smartphones and actively vet these apps for malicious content. Additionally, most major US banks will provide a link to their mobile app on their website. The FBI recommends only obtaining smartphone apps from trusted sources like official app stores or directly from bank websites.

Use Two-Factor Authentication

Since 2016, surveys of application and website users have identified that a majority



of users do not enable two-factor authentication when prompted. These users cite inconvenience as the major reason to avoid the use of this technology. Cybersecurity experts have stressed that two-factor authentication is a highly effective tool to secure accounts against compromise, and enabling any form of two-factor authentication will be to the user's advantage

Do:

Enable two-factor or multi-factor authentication on devices and accounts to protect them from malicious compromise.

Use strong two-factor authentication if possible via biometrics, hardware tokens, or authentication apps.

Use multiple types of authentication for accounts if possible. Layering different authentication standards is a stronger security option

Monitor where your Personal Identifiable Information (PII) is stored and only share the most necessary information with financial institutions.

Don't:

Click links in e-mails or text messages; ensure these messages come from the financial institution by double-checking e-mail details. Many criminals use legitimate-looking messages to trick users into giving up login details.

Give two-factor passcodes to anyone over the phone or via text. Financial institutions will not ask you for these codes over the phone.

Use Strong Passwords and Good Password Security

Cyber actors regularly exploit users who reuse passwords or use common or insecure passwords. The FBI recommends creating strong, unique passwords to mitigate these attacks. The National Institute of Standards and Technology's most recent guidance encourages users to make passwords or passphrases that are 15 characters or longer.

Do:

- ▶▶ Use passwords that contain upper case letters, lower case letters, and symbols.

- ▶▶ Use a minimum of eight characters per password.

- ▶▶ Create unique passwords for banking apps.

- ▶▶ Use a password manager or password management service.

Don't:

- ▶▶ Use common passwords or phrases, such as "Password1!" or "123456."

- ▶▶ Reuse the same passwords for multiple accounts.

- ▶▶ Store passwords in written form or in an insecure phone app like a notepad.

- ▶▶ Give your password to anyone. Financial institutions will not ask you for this information over the phone or text message.

If a Banking App Appears Suspicious, Call the Bank. If you encounter an app that appears suspicious, exercise caution and contact that financial institution. Major financial institutions may ask for a banking PIN number, but will never ask for your username and password over the phone. Check your bank's policies regarding online and app account security. If the phone call seems suspicious, hang up and call the bank back at the customer service number posted on their website.

5 Common Causes and Precautions of Computer Data Loss



✍ Data loss is a tragedy that every computer user has to suffer from at least once a couple of years. This issue is frightening and disgusting. In this article, we are going to take a look at 5 common causes of data loss and the precautions that you should take.

- ▶ **Deletion of files by mistake ..** Today, most people lose their important data due to their own mistakes. For instance, they delete their important files by mistake and they have no backups of the files. Without an iota of doubt, we delete many files every day on our computers.

Precaution: it's better if you create a backup of your important files. This way you can recover the files quickly in case you delete them by mistake.

- ▶ **Viruses Attacks ...** Virus and malware attacks is another common problems these days. And most viruses tend to corrupt our important files. As long as you are connected to the web, you can't avoid the risk.

Precaution : if you want to prevent the data loss by malware and viruses, make sure you invest in a powerful antivirus to protect your computer against virus and malware attacks. The antivirus app will give you a warning each time a suspicious activity is going to happen on your computer due to a virus.

- ▶ **Mechanical Issues ...** The failure of a hard drive is an annoying issue. Of all the hard drive issues, the mechanical issue is the most common. Typically, the issue is associated with the spindle or the head of the drive. If this happens, you have no choice but to repair the damaged components. However, don't make the mistake of doing it yourself.

Precaution: instead of opening up the drive yourself, we suggest that you take proper care. For instance, you should never drop the drive or hit it hard against a solid object. This can help you prevent a lot of mechanical issues associated with your computer hard drive.

- ▶ **Sudden Power Outages ...** You may be familiar with the term "power failure" in the world of computers. You may have experienced power outages. In case of a power failure, you may lose some important data, especially if the light goes out while you are trying to modify or compose a file. Without any doubt, the file may get corrupted.

Precaution: if you want to prevent the data loss against a power outage, you may want to make use of a surge protector. You can also use a battery or some other type of Uninterrupted Power Supply.

- ▶ **Water Damage ...** Apart from the factors given above, your hard drive may also get damaged if exposed to water. For instance, if you spill some liquid on your computer by mistake, your hard drive may get damaged. In another scenario, you may end up dropping your computer into water.

Precaution: if you want to prevent water damage, we suggest that you try to reform yourself first. This means that you should correct your bad habits. Try to keep your computer away from water.



10 Proven Ways to Make Money With Your Own Blog

✍️ A number of people own blogs but they do not know how to make money out of them. This is mainly because they do not realize how to create attention and attraction for prospective clients to fund their blogs.

A well planned and managed blog can actually offer you freedom and control over your financial future. With an effective follow-up of promises of certain blogs and following 'how-to' manuals, you can actually smile all the way to the bank. On that note, in the following discussion, we are going to look at 10 proven ways to make money with your own blog.

1. Google AdSense

Google AdSense is a very significant tool that was designed with blog and website publishers in mind. Google AdSense works with Cost Per Click (CPC) and Earning Per Click (EPC). Blog publishers will basically get paid for clicks on Ads that appear on their sites. Anyone who has created, and maintains his blogs, can essentially take advantage of this fantastic opportunity. If you really know how to use the tool to your advantage, you can generate a great deal of revenue.

2. Amazon Associates

Amazon associates is majorly an affiliate system of a program primarily involving an agreement between the advertiser (you) and the retailer (Amazon). The advertiser markets the involved and he is paid by the retailer based on an agreement. More importantly, the amazon associate will get some commission when an interested buyer clicks on a given link online and makes a purchase. If you can manage to market as many products links as possible in your blog and sell some Amazon products then it's possible that you can indeed make good money on your blog.

3. e-Books

e-Books are basically books that are in a soft copy format and can be downloaded on an internet connection. There

are a number of ways through which eBooks can be created. You can employ writers, write them yourself or even use a public domain content. There are always numerous ready buyers to buy your eBooks, regardless of your area of concentration. With your blog, you can actually be selling your eBooks and get money or you can opt to sell the eBooks for other writers and they will pay at a commission.

4. Sponsored Content

Sponsored content is generally a native advertising method through which brand-sponsored videos and articles appear on social media platforms and sites of influence and also publishers. When you have sponsored content, there are usually a number of things you need to keep in mind as you market it. Firstly, do a perfect timing for your content, tie the content with your targets audience, use high-quality content such images to add value to the content and keep the tone relatable and authentic. You can always find brand-sponsored articles from big brands and advertise it on your blog and through that, you can indeed raise a significant amount of money.

5. Contextual Ads

This is essentially a form of targeted advertising that features adverts that appear on websites, such as the content displayed on mobile devices' browsers. In a nutshell, in contextual ads, the system displays ads that are closely related to the content of your site depending on the keyword targeting. With contextual ads, you are

When talking about an online course it's essentially a method of selling what you know. It can be your skill, or any form of art, such as teaching people how to play guitar, how to bake bread or how to use a specific software. With your blog, you can sell your online course very easily.

normally paid per number of clicks. If you can get a significant number of contextual ads displaying on your blog then you can actually earn relatively good money depending on the number of clicks.

6. Banner Ads

This is an advertisement that appears on a webpage in the form of a column, bar or box. The major function of a banner ad is to promote a brand or, even more importantly get visitors from the host site to advertise on its advertiser's website. The major function of a banner is to add traffic to your site and through that, you can seal your marketing deal. The more the traffic to your blog, the better. High traffic means high income.

7. Online Courses

When talking about an online course it's essentially a method of selling what you know. It can be your skill, or any form of art, such as teaching people how to play guitar, how to bake bread or how to use a specific software. With your blog, you can sell your online course very easily. The course can be learned by many people across the globe increasing traffic to your website. Through this, you are able to make a lot of money on your blog.

8. Promote Paid Webinar or Live Event

Promotion of paid webinar basically refers to promoting a web conference, online meeting or a presentation that is held online. Live events are always advantageous to both the attendees and presenters. One consideration when it comes to promoting live events is the target audience. Through the promotion of webinar paid events, you generate traffic to your blog hence ending up being paid by your advertiser.

9. Get Paid to Write Reviews

A number of brands hire people to write reviews about them and their products. In addition to that, you always have to be honest in proving both the positive and negative reviews. Importantly, through other freelancing platforms, you can also get jobs of writing reviews for different brands. This can actually earn you good money if you are consistent in your work. All you need is to equip yourself with the proper tips.

10. Consulting Service

Consulting services basically refer to professional practices that offer expert advice within a particular field. There are many areas where you can specialize and offer advice in as much as your blog is concerned. Making money through consultancy services starts by first inventing your experience and skills. With your skill and experience, you can always earn money per project basis. Use your blog to advertise you're services and you will earn good money through consultancy.

Conclusion ... With the above-discussed ways, it's undoubtedly obvious to see ways that will earn good money from your blog. All you need is to manage, maintain and, take advantage of various opportunities to generate money from your blog.

All about Page Rank

PageRank (PR) is a mathematical algorithm that Google uses to rank pages of the websites in its search results.

As per the Google, Pagerank determines the importance of a website by counting the number and quality of links to the pages of the site. The basic assumption is that more important sites tend to receive more backlinks from other websites.

The rank value determines the importance of a particular page.

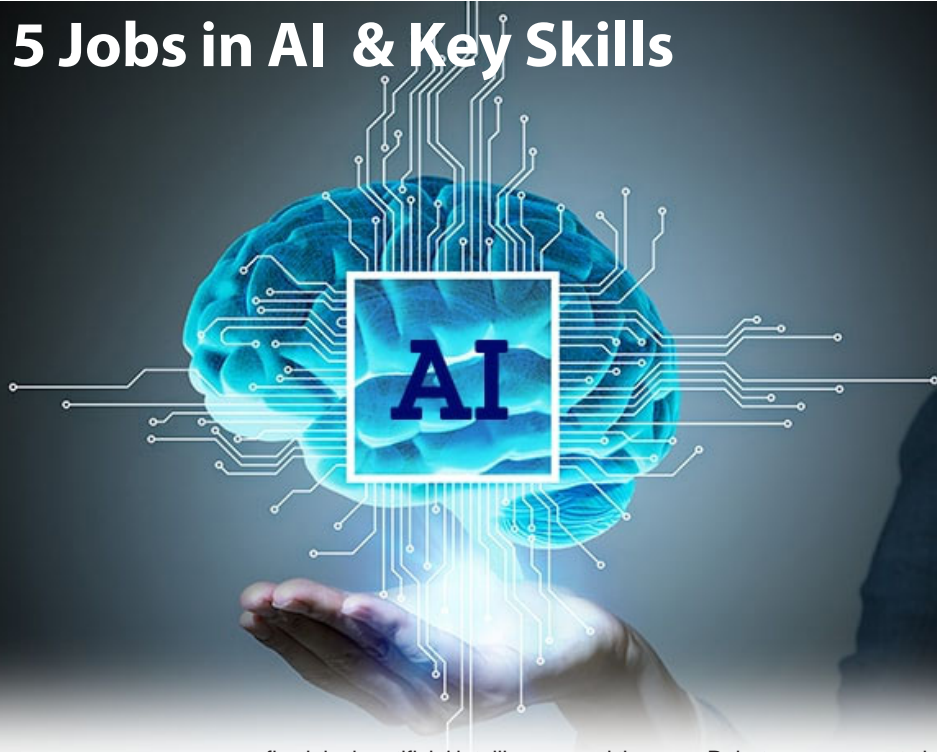
Research (from AOL's search engine logs) shows that more than 90% of the buying decisions start with a search online. And the first ten search results receive the majority (89%) of the entire click-through traffic. And the next ten results which are usually displayed on the second page receive less than 5% of the click-through traffic.


Therefore ranking on the first page is so important that companies can rise or fall due to their Google search results when customers are looking online for the products and services that they sell.

Few facts about PageRank are:

- PageRank is just one of the numerous factors that Google uses in its search result Algorithm. There are various other factors also that affects the Google's search rankings. One should focus instead on delivering quality content.
- Outbound links help the ranking of the website. Therefore they are ranking factors too.
- The algorithms are so complicated and complex that sometimes even leading search engineers working for Google don't understand them. It is almost impossible to know every bit of code because Google has made over 450 algorithm changes in one year.
- The greater the number of links on a page, the less each link's worth.
- You cannot use no-follow to control where the PageRank goes. So if you have five links on a page and two are no-followed, the PageRank calculation will still count the number of outbound links from that page to 5 even when 2 of the links are no-followed.
- Outbound links never pass the full amount of PageRank. The amount of PageRank that flows out per link is always varied. All the links pass a little less or a little more PageRank than what came into the page in the first place.
- A link from a reputed or an authority site will help increase the rankings in search engines might not be a right expectation.
- An outbound link might have a negative ranking value if it is linked to an irrelevant website.
- The entire site doesn't lose ranking when it passes PageRank. PageRank is more about the pages and the inbound links associated with those pages. So most likely, a site doesn't lose its rankings with outbound links. An important and relevant page will be able to attract attention and rank through links.
- Every page has its own importance. While considering the links on a page, there isn't any need to consider whether an outbound link is going to impact the ranking of another page negatively.
- The quality and usefulness of the web page to its users determine its importance and ranking in search engines and not the entire website.

Top 5 Jobs in AI & Key Skills



 Artificial Intelligence (AI) technology has been gaining popularity in recent years. From robots serving food in restaurants to self-driving cars, these applications of artificial intelligence can be seen in our day-to-day lives. John McCarthy, an American computer scientist who coined the term artificial intelligence, defines this discipline as the science and engineering of making intelligent machines, especially intelligent computer programs. Essentially, AI develops intelligent software and systems based on how human minds think, learn, decide and solve a problem. It enables machines to perform human-like functions by learning through experience.

While professionals across the globe are worried about robots replacing humans, a Gartner study reports that AI is an emerging field that will create 2.8 million jobs by 2020. AI is a broad term, encompassing general artificial intelligence, machine learning, expert systems, data mining and more. In today's world, AI capabilities are in great demand across industries—gaming, robotics, face recognition software, weaponry, speech recognition, vision recognition, expert systems and search engines.

If you're evaluating career options in this emerging field, look at these top

five jobs in artificial intelligence and the skills that you'll need to transition into these roles.

1. Machine Learning Engineer

One of the most sought-after jobs in AI, machine learning engineers must possess strong software skills, be able to apply predictive models and utilize natural language processing while working with massive data sets. In addition, machine learning engineers are expected to know software development methodology, agile practices and the complete range of modern software development tools right from IDEs like Eclipse and IntelliJ to the components of a continuous deployment pipeline.

Preferred Qualifications :

Hiring companies prefer candidates holding a master's or doctoral degree in computer science or mathematics with working knowledge of modern programming languages like Python, Java, and Scala. Professionals with strong computer programming skills, expert mathematical skills, knowledge of cloud applications and computer languages, excellent communication and analytical skills and certifications like machine learning are usually preferred by these organizations.

2. Robotic Scientist

Robots can automate jobs but they require programmers working behind the scenes to ensure they function well. Robotic science is used for multiple functions from space exploration, healthcare, security to many other scientific fields. Their primary function is to build mechanical devices or robots who can perform tasks with commands from humans. Other necessary skills required for this role include writing and manipulating computer programs, collaborating with other specialists and developing prototypes.

Preferred Qualifications :

A bachelor's degree in robotic engineering/mechanical engineering/electro-mechanical engineering/electrical engineering is a basic prerequisite. Companies also look for professionals with specializations in advanced mathematics, physical sciences, life sciences, computer science, computer-aided design and drafting (CADD), physics, fluid dynamics and materials science and related certifications.

3. Data Scientist ...

Data scientists collect, analyze and interpret large amounts of data by using machine learning and predictive analytics to gain insights beyond statistical analysis. They should have expertise in using Big Data platforms and

tools including Hadoop, Pig, Hive, Spark, and MapReduce. Data scientists are also fluent in programming languages including structured query language (SQL), Python, Scala, and Perl, as well as statistical computing languages.

Preferred Qualifications :

Data scientists are highly educated, with the majority holding master's or doctoral degree, though an advanced degree in computer science is preferred, it is not a prerequisite. The most desired technical skills are in-depth knowledge of SAS and/or R, Python coding, Hadoop platform, experience working on cloud tools like Amazon's S3 and the ability to understand unstructured data. Non-technical skills required include strong communication and analytical skills, intellectual curiosity and business acumen.

4. Research Scientist

A research scientist is an expert in multiple artificial intelligence disciplines including machine learning, computational statistics, and applied mathematics. In particular, these areas include deep learning, graphical models, reinforcement learning, computer perception, natural language processing and data representation, graphical models, reinforcement learning, computer perception, natural language processing and data representation.

Preferred Qualifications :

A master's or doctoral degree in computer science, or in a related technical field or equivalent practical experience is the basic requirement for this role. Companies also tend to prefer professionals who possess skills such as parallel computing, artificial intelligence, machine learning, knowledge of algorithms and distributed computing and benchmarking. Alongside these qualifications, an in-depth understanding of computer architecture and strong verbal and written

"Business intelligence developers are in high demand. Their primary job is to analyze complex data and look for current business and market trends, thereby increasing profitability and efficiency of the organization".

communication skills are recommended for those interested in this field.

5. Business Intelligence Developer

Business intelligence developers are in high demand. Their primary job is to analyze complex data and look for current business and market trends, thereby increasing profitability and efficiency of the organization. Not only are they masters of strong technical and analytical skills, but they also have sound communication and problem-solving skills. They are responsible for designing, modeling, building and maintaining data for complex, extensive and highly accessible cloud-based data platforms.

Preferred Qualifications :

A bachelor's degree in computer science, engineering or a related field is required; or a combination of certifications and on-the-job experience are preferred for this role. Candidates with experience in data warehouse design, data mining, knowledge of BI technologies, SQL queries, SQL Server Reporting Services (SSRS) and SQL Server Integration Services (SSIS) and popular data science certifications are preferred.

The job opportunities available by the advent of artificial intelligence are only going to grow as the technology continues to innovate. Experts from Gartner predict, "AI will create more jobs than it eliminates." Each role, however, requires education and training to fulfill the needs of the industry. Raj Mukherjee, Senior Vice President of Product at Indeed, puts it into perspective, "There are certain standard technical requirements, such as a computer science degree or programming skills. A background in programming languages like Python, Java, C/C++, and experience in artificial intelligence, machine learning or natural language processing are some of the top skills employers look for in AI applicants."

For those of you who are planning to pursue a spot in the AI field, you must start today by preparing yourself with the tools needed to execute the job successfully. Obtaining certifications in domains like machine learning and AI is a great place to start and with the right education, the opportunities are endless.



With so many of us using social media today, sites like Facebook, Twitter, and LinkedIn make perfect targets for scams.

Here are our top 10 tips to stay safe on social media:

- » Use a strong password. The longer it is, the more secure it will be.
- » Use a different password for each of your social media accounts.
- » Set up your security answers. This option is available for most social media sites.
- » If you have social media apps on your phone, be sure to password protect your device.
- » Be selective with friend requests. If you don't know the person, don't accept their request. It could be a fake account.
- » Click links with caution. Social media accounts are regularly hacked. Look out for language or content that does not sound like something your friend would post.
- » Be careful about what you share. Don't reveal sensitive personal information ie: home address, financial information, phone number. The more you post the easier it is to have your identity stolen.
- » Become familiar with the privacy policies of the social media channels you use and customize your privacy settings to control who sees what.
- » Protect your computer by installing antivirus software to safeguard. Also ensure that your browser, operating system, and software are kept up to date.
- » Remember to log off when you're done.

Top Five Social Media Scams



We're wired to be social creatures, and sites like Twitter and Facebook have capitalized on this to great success. According to its COO Sheryl Sandberg, Facebook draws 175 million logins every day.

But with this tremendous popularity comes a dark side as well. Virus writers and other cybercriminals go where the numbers are — and that includes popular social media sites. To help you avoid a con or viral infection, we've put together this list of the top five social media scams.

Social media scams can quickly spread across social platforms like Twitter and Facebook. Understand how they work and take steps to protect yourself.

» How social media scams work

Social media scams are usually cunningly crafted by a scammer to appear genuine, using official brand logos, made up T&Cs and including a link to enter your details.

Unbeknown to the victim, clicking on these links sends your personal information to third parties, while also triggering the share feature to your connections, sometimes with an added status message. Friends and family are then more likely to fall for the scam as they are likely to see the message and link as a trusted endorsement.

» Chain Letters

You've likely seen this one before — the dreaded chain letter has returned. It may appear in the form of, "Retweet this and

Bill Gates will donate \$5 million to charity!" But hold on, let's think about this. Bill Gates already does a lot for charity. Why would he wait for something like this to take action? Answer: He wouldn't. Both the cause and claim are fake.

So why would someone post this? Good question. It could be some prankster looking for a laugh, or a spammer needing "friends" to hit up later. Many well-meaning people pass these fake claims onto others. Break the chain and inform them of the likely ruse.

» Cash Grabs

By their very nature, social media sites make it easy for us to stay in touch with friends, while reaching out to meet new ones. But how well do you really know these new acquaintances? That person with the attractive profile picture who just friended you — and suddenly needs money — is probably some cybercriminal looking for easy cash. Think twice before acting. In fact, the same advice applies even if you know the person.

Picture this : You just received an urgent request from one of your real friends who "lost his wallet on vacation and needs some cash to get home." So, being the helpful person you are, you send some money right away, per his instructions. But there's a problem: Your friend never sent this request. In fact, he isn't even aware of it. His malware-infected computer grabbed all of his contacts and forwarded the bogus email to everyone, waiting to

see who would bite. Again, think before acting. Call your friend. Inform him of the request and see if it's true. Next, make sure your computer isn't infected as well.

» Hidden Charges

"What type of STAR WARS character are you? Find out with our quiz! All of your friends have taken it!" Hmm, this sounds interesting, so you enter your info and cell number, as instructed. After a few minutes, a text turns up. It turns out you're more Yoda than Darth Vader. Well, that's interesting ... but not as much as your next month's cell bill will be.

You've also just unwittingly subscribed to some dubious service that charges \$9.95 every month.

As it turns out, that "free, fun service" is neither. Be wary of these bait-and-switch games. They tend to thrive on social sites.

» Phishing Requests

"Somebody just put up these pictures of you drunk at this wild party! Check 'em out here!" Huh? Let me see that! Immediately, you click on the enclosed link, which takes you to your Twitter or Facebook login page. There, you enter your account info — and a cybercriminal now has your password, along with total control of your account.

How did this happen? Both the email and landing page were fake. That link you clicked took you to a page that only looked like your intended social site. It's called phishing, and you've just been had. To prevent this, make sure your Internet security includes antiphishing defenses. Many freeware programs don't include this essential protection.


» Hidden URLs

Beware of blindly clicking on shortened URLs. You'll see them everywhere on Twitter, but you never know where you're going to go since the URL ("Uniform Resource Locator," the Web address) hides the full location. Clicking on such a link could direct you to your intended site, or one that installs all sorts of malware on your computer.

URL shorteners can be quite useful. Just be aware of their potential pitfalls and make sure you have real-time protection against spyware and viruses.

Bottom line : Sites that attract a significant number of visitors are going to lure in a criminal element, too. If you take security precautions ahead of time, such as using antivirus and anti-spyware protection, you can defend yourself against these dangers and surf with confidence.

Top 5 Signs, Time to Replace Your Phone Battery

 No electronic products last forever and same is the Mobile phone Batteries! As you charge and discharge your battery, it degrades and over time, you get less battery life from a full charge. Eventually, the battery—or the device—needs to be replaced. Luckily, there are several ways to determine if the cell phone needs a new battery. Let's start to explore!

» The Phone is Overheating Quickly :

It is known that the batteries generate heat as they are charged. However, the batteries are optimized to manage the heat and shielding it from becoming noticeable. If it starts becoming too hot to touch your phone even on moderate usage pretty often, it means its time to look for a battery replacement.

» Lacking of Power :

Perhaps the most obvious sign of a failing cell phone battery comes when the phone simply refuses to work. In this case you will not be able to hear any sounds when you press the keys and the display screen will be dark. Hold down the Power button on your cell phone for a few seconds or even a minute. If there is any life left in the battery, the phone should eventually turn on. If nothing happens, make sure the battery contacts are clean. If the contacts are dirty or dusty, this can disrupt the charging process. If the

contacts are clean and holding down the power button for a period of time does not revive the phone, the battery is failing.

3. The Phone is Dead:

This may be an obvious one. Either you accidentally damaged your phone by dropping it or dunking it in water for too long, or the battery is dead. If you've eliminated the first, check to see if it shows no sign of power - nothing lights up, no sound. If the phone shows no signs of life after charging with a reliable charger, it's time to call it: your battery is dead. There is a good chance that the battery may need to be replaced.

4. Checking for a Bulge in the Battery:

It is easy to spot a difference in the battery. Sometimes, when a battery goes bad, the internal cells rupture, and cause a bulge to appear in the battery. You see this when you hold the battery up or see a bulge on the casing. Additionally, a bulge makes it able to spin like a top when placing the battery on a flat surface. If the battery has bulged, you need to take it to the vendor for advice if it has to be replaced. Don't use the damaged battery as it might cause harm to the circuitry of the phone.

5. Checking on the Battery Life:

You need to diagnose the battery's health by monitoring how fast the battery level drops. You shouldn't

notice more than two percentage of the battery level instantly. If the battery level drops from full charge to zero in a few hours even while you haven't used the phone for intense activities, you need to consider replacing the battery.

How To Improve Smart Phone Battery Life :

- ▶ How to extend the life of the battery on your mobile phone....
- ▶ To extend the battery life of your phone, follow the instructions below:
 - ▶ Turn off Bluetooth when you do not need it;
 - ▶ Please turn off scanning, turn off Show wireless LAN availability in the wireless LAN settings when you are not using Wi-Fi;
 - ▶ The brightness of the screen may affect the standby time of the battery. In the display settings, you can change the delay (standby time) and adjust the brightness;
 - ▶ Let applications run in the background increase battery power consumption, please close the application you do not use;
 - ▶ Please disable the vibrate function of your mobile phone, and just use the ringtone to extend the battery life;
 - ▶ Please try not to let apps, pictures, video play in the background. If the battery runs out quickly, even if no function is consumed, the battery may wear out and you must replace it with a new battery.



Lack of Skills Threatens Digital Transformation

Contributor: Scott Engler | Source: Gartner

As the COVID-19 response accelerates the speed and scale of digital transformation, a lack of digital skills could jeopardize companies with misaligned talent plans.

Even before there was a coronavirus pandemic, boards ranked digital/technology disruption as their top business priority for 2020 — followed by obtaining the talent needed to execute tech transformation. But COVID-19 has escalated digital initiatives into digital imperatives, creating urgent pressure on HR leaders to work with their CEO, CFO and CIO to rethink skills needs as business models change at light speed.

It's no easy task for this cohort to identify and acquire the digital skills their organization needs to pursue digital transformation as imagined post-COVID-19. And now companies must press forward under a new reality: Technology skills are no longer highly centered in IT; they need to be "marbled" across organizational functions and businesses and coupled with soft skills to achieve transformation success.

Consider the sales rep: Gartner TalentNeuron data shows that technology industry leaders like Facebook, Apple, Amazon, Google and Microsoft look for a digital skillset that includes engineering, digital transformation, Microsoft Azure, security, computer science and tech infrastructure. But it's not just sales reps nor tech leaders who are affected; digital skills are now part of almost every role.

Yet most companies are flying "data blind" with regard to the skills they need for transformation and the supply, demand, availability and location of those skills. Fifty-three percent of respondents to a recent TalentNeuron survey said that the inability to identify needed skills was the No. 1 impediment to workforce transformation. Thirty-one percent reported that they have no way to identify market-leading skills.

Digital transformation speeds up and spreads

By some estimates, response to the pandemic has fast-forwarded digital adoption by five years. One result of this "digitalization at scale and velocity" is massive skill shifts. The shift in skill needs was already a challenge, but more than 58% of workforces report skill transformations since the onset of the pandemic.

Many leaders are ill-equipped to manage the fallout. The very business leaders who already lagged in making the digital leap

are often the same ones we're depending on to hire and develop future-forward strategies to cope with this change.

If senior leaders can't solve this puzzle, they won't be able to deploy and align the right type or amount of skills to address the shifts in work trends, processes and organizational structures that fuel digital transformation.

'Digital' doesn't just mean 'remote'

Often lacking is critical understanding of how digital impacts the business, and how to effectively plan and deploy the critical skills needed to fuel the reimagined business model.

As one CEO recently told me: Every company is going to have to transform digitally. He described the need to invest in this moment of crisis, saying "Everyone's going to have to adapt new ways of creating and delivering value." This applies to customer relationships, sales and services, marketing and commerce, collaborating and reskilling workers, and more.

It's important to note how radically and broadly digital capabilities will be needed. We've become used to remote work and remote transactions, but "digital" doesn't just mean "remote."

As businesses reinvent themselves, some will focus on digital initiatives that improve productivity and reduce costs; others will focus on existing or new digital commerce and digital revenue sources. You have to plan for what digital evolution means to your business model, not base your plans on how work is being done now.

Data shows demand for digital skills keeps expanding

In 2019, data from Gartner TalentNeuron already showed an outsized number of technologists being hired outside of IT. That trend is only accelerating as organizations demand digital skills far beyond the IT function and deep into other areas of the business.

You can see this in the figure below, which shows data on job postings by non-technology companies tied to skills around artificial intelligence, robotic process automation and data science/analytics.

Catching up with tech companies on critical skills

The pandemic response has already driven radical and lasting change in work trends, including shifts around remote and contingent work and critical skill needs. But as executive leaders reset their digital business strategy, the talent strategy will need

to serve the chosen end state. Companies that were poised for digital transformation before COVID-19 are quickly distancing themselves from analog companies and the rest are scrambling to catch up.

Even if nontechnology companies don't need employees to be quite so digitally literate as the tech giants, they will need to identify their requisite skills and prioritize a way to acquire them. This is especially critical if they hope to unlock the value of the competitive advantage embedded in the reimagined business model.

Ways to redeploy talent resources

Whatever the value proposition is for customers and other external stakeholders, every organization will need employees to function in a more digitalized environment — where decision making and workflows are constantly changing.

Even before COVID-19, HR leaders rated the emergence of new tasks as their top disruptors and commonly said they struggled to plan for future talent needs. The pandemic has confirmed what many already knew: Legacy ways of working are outdated.

Talent resources are increasingly misaligned with work processes and organizational structures. And the traditional approach to allocating talent — using episodic overhauls and adjustments — simply isn't agile enough for today's fast-changing conditions.

The way work is designed diverges over time from the way it actually gets done, and now that's happening even more quickly, so organizations need to:

- » Embed agile work design assessments into broader talent management activities.
- » Break roles and projects into skills so you can begin to identify the work model that best meets the skills requirements. Then you have options. For example, to make up for a lack of a given digital skill, you could borrow from another department, do an interdepartmental talent swap, hire a freelancer or crowdsource capabilities.
- » Decide the fate of different roles as the environment evolves, unbundling resources to adapt to devolved decision-making authority.

Consider the options for roles at risk from artificial intelligence and automation:

- » Preserve the role as is, but stay ahead of the curve. Forecast what changes can still impact the role and prepare a strategy plan for how to successfully handle potential transitions.
- » Enhance the existing role with new or improved capabilities so it can adapt proactively to the changing work landscape.
- » Rightsize the role to realign with what's required in a new environment.
- » Eliminate the role when it runs an unavoidable risk of automation. Eliminating the role doesn't necessarily mean eliminating the talent.
- » Predict an entirely new role to replace an antiquated existing role.
- » Ultimately, talent planning has to move resourcing closer to the end-user, making it easier for employees to act on changing needs and helping to keep resources from getting stuck in less-productive projects.

Advantages of Cloud Storages

Utilizing an outer drive is the most generally utilized approach for having reinforcement stockpiling. The general population who mull over making utilization of distributed computing for this reason regularly think about whether the innovation is justified regardless of the exertion. Clients of the framework guarantee that there is no motivation behind why anybody must abstain from utilizing this framework as it guarantees different extra points of interest when contrasted with the ordinary techniques.

The way that one needs to spend an infinitesimal measure of cash each month for the utilization of cloud information stockpiling is one explanation behind potential clients to be reluctant. Notwithstanding, the accompanying advantages of the innovation are reason enough to guarantee that this cash spent is well justified, despite all the trouble.

Extensive storage space: The most fundamental preferred standpoint of utilizing the cloud is that one can store any measure of information, which is outlandish while utilizing drives. Additionally, the framework is to a great degree simple to use as the record is made in minutes, instead of the time and exertion spent on going looking for an outside drive.

No Physical presence: Once you have put away your information on the cloud, it turns into the obligation of the supplier to stress over its upkeep. Rather than purchasing and putting away those various outer drives, one just needs to remain associated with the web keeping in mind the end goal to get to the put away information.

Convenience of automatic backup: The clients of distributed computing don't need to try guaranteeing that they have associated the outside drive to their PCs and that they take reinforcements at general interims. The settings on the cloud framework can be changed according to the client's inclination with respect to whether the reinforcement ought to be taken various circumstances in a single day or once consistently. The main clear essential for the framework to be moved down is that the web ought to be associated and everything else is dealt with.

Easy restoration: In regular conditions, recovering and reestablishing a hard drive from moved down information is a long and awkward process which requires the administrations of a PC professional. The cloud clients are saved from any such burden as this reclamation procedure is made straightforward and brisk. On the off chance that at all the clients still have questions about taking care of this all alone, they can simply look for assistance from the suppliers and they will gladly oblige.

For such huge numbers of administrations, the little expense charged by the supplier ought to barely be a killjoy. One can simply be on the watch out for rebates and offers that are offered by cloud suppliers for new customers which chop down the expenses to an absolute minimum.

Gartner Identifies Six Health and Safety Factors Customer Service and Support Leaders Must Consider When Planning the Return to the Office.

Service and Support Leaders Must Prioritize Employee Well-Being in Preparation for Post COVID-19 Operations

As governments start to lift stay at home orders, Gartner, Inc. has identified six health and safety factors service and support leaders must consider when employees return to the office. Employees must be confident that their well-being is prioritized when facilities are reopened, and staff are moved back to the office or current on-site staff capacity is increased.

A recent Gartner, Inc. survey found that social or physical distancing arrangements was the top workplace standard to have in place when employees return to the office, followed by adequate personal protective equipment (PPE) and safe work playbook (or equivalent).

“Service and support leaders planning to return employees on-site have a host of factors to consider before doing so,” said Deborah Alvord, senior director analyst in the Gartner Customer Service and Support Practice. “These range from assessing current office conditions, implementing social distancing guidelines and potential facility upgrades. A successful return to work program will alleviate staff fears and concerns, and ease the transition of going back to the workplace.”

Return to Workplace Standards

Gartner recommends that service and support leaders consider the following factors in their return to work program.

1. Current office conditions: Review each area of the office, such as the break room, meeting space, rep workspace, collaboration space, restrooms and dining area to identify where changes need to be made to adjust for social distancing and proper hygiene requirements.

2. Employee hygiene modification: Distribute hygiene

guidelines to employees and provide training to employees returning to the office on hygiene modifications that must be followed.

3. Social distancing modification: Understanding the impact of new social distancing guidelines on office space is essential for informing employees’ return to work strategies. Assess whether social distancing guidelines will reduce maximum office capacity and evaluate the portion of staff that may have to continue working remotely.

4. Facility requirements and adjustments: Conduct a thorough assessment of the work environment and make needed adjustments. Organizations who do not own their facilities should partner with the property owner to assess the environment and develop a plan.

5. Return to work criteria: Create a list of criteria using state, local and federal HR and health guidelines to identify those employees that are eligible for return to the office and those that are at higher risk. Take into consideration employees who volunteer to return to the office, employees who live closest to the office and wouldn’t have to take public transportation and high-risk groups.

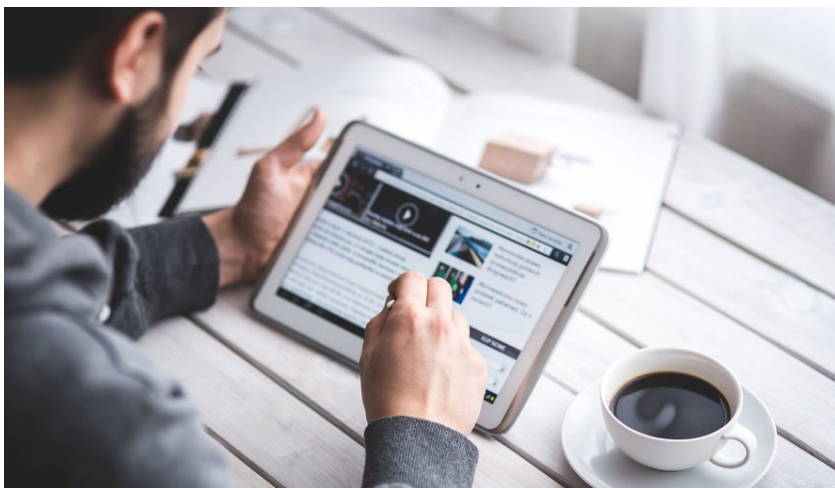
6. Communication and management changes: Ensure communications regarding return to the office are sent weeks in advance of implementation to allow employees to make accommodations and adjust. This should include the changes made to the office to prioritize employee health and well-being, along with how reintroduction of staff to the office will occur.

“While assessing the success of a return to work program, service leaders should also gather continuous employee feedback,” said John Quaglietta, senior director analyst in the Gartner Customer Service and Support Practice. “This helps identify gaps in the current policies, provides an opportunity for organizations to address concerns directly and should be used to adjust the return to work phases.”

Gartner Identifies Six Health and Safety Factors



How To Make Money Online Selling Other People's Products



» What is Affiliate Marketing

Affiliate marketing is one of the oldest forms of marketing wherein you refer someone to any online product and when that person buys the product based on your recommendation, you receive a commission.

Many online companies who sell products such as shoes, web-hosting spaces, or some other service, usually offer an affiliate program. You can simply sign up for the program and get your unique tracking link. Now, whenever you are writing about their product, you can simply use this special tracking affiliate link to recommend the company's site.

If your readers buy anything, you will get a commission.

Every affiliate program has a set TOS. For example, many of them offer a 60-day cookie period, which means that if a visitor uses your special affiliate link to land on the sales page of the site and buys something within the next 60 days, you will be entitled to the sale's commission.

To make money online don't have to create, own or stock your own product. You can direct potential customers to websites already selling products that have been created by other people and if somebody buys the product following your referral to that website, the product owner will pay you a commission.

The product owner also organizes the customer payment, delivery and fulfillment of the product. This is called affiliate

marketing and it's your job as an affiliate to connect prospective customers with products or services that they're looking to buy.

» So how do you get started?

Choose Your Audience

Before you start to look for products you can sell, you have to determine your target audience or niche. What problems do the audience in your chosen niche want to resolve? The affiliate products you promote should offer the solutions they're looking for. You can find a huge number of products to sell from affiliate marketing companies like Amazon, CJAffiliate, ClickBank and JVZoo.

» Start Small

You won't make hundreds of thousands in a single day. Start small and keep improving your online reputation. Develop and provide high-value content on your website and social media. There are affiliate programs that do not require a website, but your own website makes it possible for you to concentrate on

being authentic so that you come across as being reliable and professional.

» Build An Email List

Concentrate on developing an email list of prospective customers from your website and social media accounts. You can send emails to your list whenever you want. This is the most effective way you'll have people buying the products and services you recommend.

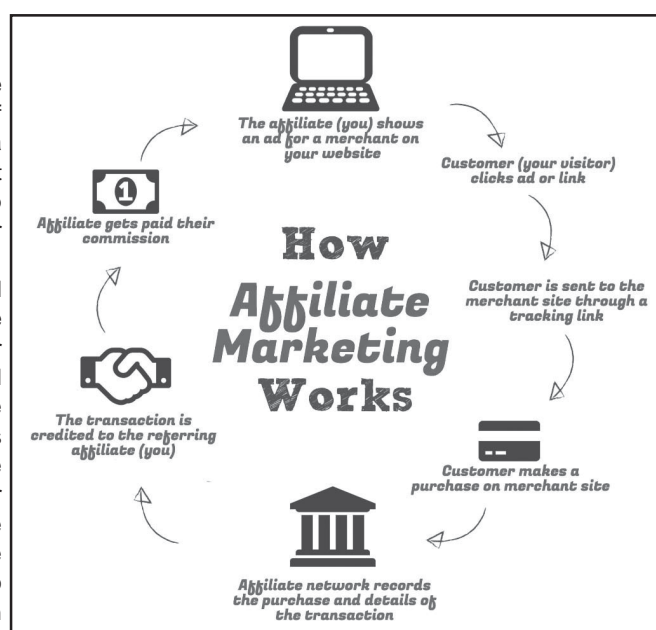
» Treat It Like A Business

Even if you only work it part-time you need to treat it like a real business and not something you play around with. It's okay to play around at the beginning to see if it's right for you and it's a good way to learn. But eventually, if you want to create a real online business you'll have to treat it that way.

» Think 'Telling' Not 'Selling'


Be helpful, friendly and care about the things you promote. Look at it as more about 'telling' rather than 'selling'. When you put it in the perspective of helping people find what they need or want, you take the strain off yourself to be continuously selling. This will allow your efforts to flow from genuineness rather than looking overeager in trying to make money.

Companies are happy to pay commissions to people just like you, in return for selling their products and services. You have the potential to make a great income when you choose the right niche, stay committed, and understand your audience.



These are the 5 types of data that analytics analyzes



 Businesses are using analytics to build strategies, as well as, to make short-term decisions by leveraging different types of big data through the use of appropriate methods of data collection and analysis.

Big data enables organizations to monitor both big picture trends and subtle changes in their respective spaces and industries and gives them insights to enhance decision-making and problem-solving capabilities. Knowing the different types of big data that can be gathered and analyzed using analytics will help businesses realize the potential impact that can be achieved with the technology and give businesses an improved sense of direction for their big data initiatives.

Following are five major types of big data that organizations can use:

Types of Big Data

» Customer data

The most successful businesses are built around their consumers. Creating a customer-centric business requires knowing the customers well. To know their customers well, businesses gather and analyze all the data they can find on their customers, such as demographics, occupation, preferences, etc. Big data not only enables the collection and interpretation of data on a macro level but also allows businesses to know more about individual customers and their preferences. All of this helps a business make broad product-centric changes, while also enabling them to personalize customer

interactions. A majority of this data is structured, and most of it is gathered from the customers themselves, and stored with their consent.

» Social media data

Businesses, including the traditional corporations, are beginning to use social media as one of their primary marketing channels. Social media is not only an excellent way to reach the existing and potential customers, but also to get feedback from them. Social media content such as posts, tweets, comments, and pictures relating to brands and their products can be analyzed using big data analytics, by businesses to understand general market sentiments surrounding their offerings. It also helps businesses to catch on to trends that may help them to market their products better. This also enables marketers to gain insights into customer behavior. The different types of big data collected from social media are highly unstructured and require natural language processing capabilities to categorize social media chatter.

» Operational data

Operational data is the data relating to an organization's processes. If it's a manufacturing company, the operational data encompasses all the information on the manufacturing operation, such as the data related to the manufacturing equipment, the performance and maintenance data of all the equipments, inventory data, cycle times, etc. Analyzing

this information using big data analytics ensures the maximization of operational performance by enabling the businesses to respond to any changes that may impact the output, such as machine breakdowns. Analyzing different types of big data can also enable manufacturers to make long-term changes to their systems and to make strategic plans. Operational data is mostly structured.

» Employee data

Although technology plays a significant role, people are the primary driving force of any organization. Running a successful business involves making the most of the human resources available. Businesses monitor and analyze different data points relating to their employees to improve performance and increase employee engagement through big data. Big data can be used to evaluate the performance of different employees and assess their training needs. It can also be used to provide highly individualized training to the employees based on their needs. Analyzing qualitative data regarding employee behavior helps assess employee fitness for appraisal and promotions. Monitoring employee engagement by analyzing different types of big data for individual employees, including social media data, can help businesses ensure high employee retention.

» Market intelligence data

Making strategic business decisions, regarding the introduction or discontinuation of a product, making a major product upgrade, pricing, or acquisition and merger require a large volume of both historical, as well as, real-time data. Big data analytics is used by businesses to gain market insights such as supply-demand trends, competitor analysis, and similar external data to make optimal decisions. Market intelligence data can be a mixture of structured and unstructured data and might require data science expertise to decode and leverage.

In addition to these five types of data that organizations can analyze for improving business performance, there are many others that can be leveraged to achieve substantial growth. Some types of big data can be specifically useful for certain businesses, based on their market and offerings. Business and technology leaders should recognize their specific big data needs and identify the sources of big data available to them.



These 3 technologies play an important role in enhancing Cybersecurity

by Naveen Joshi
Founder & CEO - Allerin, Mumbai

✍ When we go online, we leave traces of our data. We would never want our data falling into the wrong hands. Organizations that gather our data recognize this as a customer-centric and regulatory requirement; thus spending a lot of time and money to take active measures for enhancing cybersecurity.

The craze for accelerating innovation, productivity, and revenue growth has compelled various organizations to embrace digitization. Business leaders in organizations are actively seeking new ideas to attain success in their business. Companies have finally recognized the driver for achieving digitization - data. They aim to collect, access, analyze, and utilize tons of data that come from various sources in different formats. By interpreting the received data using big data analytics, they can uncover the 'otherwise difficult to recognize' patterns, which can improve their business altogether. It is true that organizations always aim to use our data for a useful purpose, but there are several criminal organizations eagerly waiting to steal our information, and use it for unintended activities.

Due to the news on data breaches that regularly appear in the headlines, organizations are now investing a lot of their capital to secure their assets from

hackers. Organizations are behind identifying the right method to curb this rising issue. By building a security policy and governance model, companies can limit the access of the data to only employees who are associated with the project. But, along with this, companies should also capitalize on one or more of these technologies for ensuring cybersecurity at an optimum level.

» Big Data Analytics

With the help of data, organizations are clocking revenue growth like never imagined. But, we have also seen how this data is causing a risk of cyber threats worldwide. Now, what if we tell you that the collected data could solve this risk? Big data analytics can sift through various types of data, historical or real-time, analyze it, and give information on cyber resilience.

» Blockchain

The credentials that we use to perform online monetary transactions are recorded somewhere in the database of financial services. The storage infrastructure that these financial services use is typically centralized. But now, the case is not the same. The incredible attributes of blockchain help to secure the data from cyber threats. By using blockchain, organizations can store the data in a decentralized ledger on a blockchain network. Any access, any share, or any addition to the data on a blockchain ledger



requires validation first. The concerned participants on the blockchain network are required to enter the key (combination of private and public keys) before they wish to record any new data, access or modify it. Practically, it is not so easy for hackers to decode the keys. Hence, blockchain provides companies with a secure way to store their digital assets, thereby ensuring cybersecurity.

» Artificial Intelligence (AI)

Cybercriminals are increasingly targeting organizations for stealing their digital assets. To counter this, AI can play a prominent role in ensuring cybersecurity. By training the AI algorithm with the right data on historical threats, the model can give accurate information on proactivity of hackers. Effective solutions can then be built after gaining actionable insights on activities of hackers.

We know that today's modern technologies have helped us in many ways. But, the way these technologies are extending their helping hand to curb cyber activities is just incredible!



10 things you should know about Analytics related Career

In the last 2 years, a lot of people (beginners, transitioners) asked us how do I start my career in data analytics and similar questions. We, then started writing articles on these topics and got overwhelming response from the readers.

We bring you the curated list of all the articles based on career related suggestions and knowledge. These articles will help you to get acquainted with the steps that you must take if you are planning to enter data analytics industry.

If you are still facing any issue in your career, feel free to get in touch with us at queries@analyticsvidhya.com and we commit to respond you back within 24 hours.

Below are the list of articles which can help you to know more about career in analytics:

» How to start a career in Business Analytics?

This article will guide you through a stepwise approach to learn about how to begin your career in business analytics. Lately, a lot of folks have developed affinity for business analytics mainly because of two reasons: 1) It is a lucrative industry 2) passion for numbers/quantitative skill set. We have revealed the sets of tips which can help to choose this path.

» All you need to know to start a career in Business Analytics

There are a lot of things one should consider before making a mark in business analytics domain. Such as, he/she should learn about what part of business analytics suits the best, what sets of skills, tools,

techniques would be the best suited for his caliber. In this article, we have listed all the possibilities which should be considered for a business analytics career.

» How to become an analytics rockstar?

Lately, we received a lot of queries on how to become an awesome analyst. An awesome analyst is defined by the sets of work he can perform with great ease. It generally involves having a good grip on the concept you know of. Here is the knowledge of how you can become an analytics rockstar.

» Tips to prepare outstanding CV for Data Science roles

Curriculum Vitae marks the first impression of your candidature on the hiring team, even before you personally meet them. More than 50% of every interview success is driven by how flawlessly your resume has been built. In this article, we have discussed the tips to help you make an awesome CV for job interviews.

» How freshers can ace interviews for Business Analytics roles?

The biggest roadblock for a fresher to enter in a industry is 'clearing job interviews'. Freshers usually struggle in this stage due to lack of guidance and smartness. Here we have revealed the list of smart tactics which can help you to ace in your job interviews.

» How can I become a data scientist (business analyst)?

This has been one of the hottest topic on our website in the past 2 years. Data

Scientist is known to be sexiest job of 21st century, reckoned by Harvard Business Review. In this article, we have stated the road map which we recommend to all our readers to follow for becoming a data scientist.

» Should I become a data scientist (or business analyst)?

If you are inclined towards business analytics but still you are in dilemma if you can succeed or not, this article is a must read for you. This will make you aware, considering your current set of skill sets, if you are a fit to become a data scientist.

» Starting a big data analytics practice? Answer these 5 questions first.

Ever tried to learn about big data analytics? Here are 5 questions to challenge your status quo, which will then help you evaluate the set of knowledge you possess.

» Taking a new job in analytics? Ask these 5 questions first!

Are you looking for a new job in analytics? Here are the 5 questions that you should ask yourself before making the next move. These questions will help you reflect on your decision and its consequences.


» Planning a late career shift to analytics/big data? Better be prepared!

Lately, people have started embracing data analytics for being one of the lucrative industry today. A lot of IT professionals, marketing, finance professionals ask us how to begin the career in analytics. Here is a list of some essential points that should be kept in mind before making this shift.



These 4 big data applications are really cool..!

Technology is made for both, the usual and the unusual. While we have exploited it for major issues in the commercial domain, there still remain a lot of unexplored areas that analysts are now applying big data applications to, which are cool as well as purposive

 In the words of Andrew McAfee, 'The world is one big data problem.' From the manufacturing industry to the legal industry, big data applications have revolutionized the way we gather, process, and study data. However, along with these corporate solutions that technology provides, big data analysts have now started advancing into developing unusual solutions for the common man, like determining the best routes to work or finding the fruit tree nearest your house.

Big data applications

» Big data for medical research

Collating medical data for research is experiencing a new trend with big data analytics. Apple's new application, Research Kit, is exclusively developed to collect medical data from iOS devices with the user's consent. Designed mainly for common medical problems like asthma and diabetes, the application was upgraded to collect data related to breast cancer, cardiovascular diseases, and Parkinson's symptoms. The application gathers data either from the advanced sensors that the iOS devices have or from other health apps installed on the device. The data collected undergoes predictive analysis and clustering algorithms and is readied for medical research by students and doctors.

» Big data for foraging fruits

Big data applications are now making natural produce available for urbanites. The website, Falling Fruit.org, for instance, is helping the urban population locate the nearest agricultural and local produce directly from the trees around them. The site collates data from the US Department of Agriculture and municipal tree inventories to integrate maps with street tree databases. This data is then processed to create interactive maps and graphs that point out the location of the nearest fruit trees in a city. The website recognizes a user's location and lists all the sources of fresh fruit available in the vicinity.

» Big data for skiing resorts

Ski resorts are popularizing the application of big data for reducing wait times and studying resort statistics with predictive analysis. RFID tags are installed in skiing tickets to keep track of skier movements. The information collected from the tags is used to determine popular routes for skiing by reading the most opted skiing routes.

The data can be processed to give insights into the duration of individual skiing cycles, the frequency of the skiers around the year, and the busy hours of the day. Mathematical models are then designed to analyze this data and wait time, pricing, and skiing schedules can accordingly be decided to engage more people in the sport.

» Big data for product marketing

Another unusual application of big data is its use in social physics for answering plain-language business queries. An MIT initiative by Alex Pentland and Yaniv Altshuler, Endor, is a predictive analysis platform that allows a user to enter a raw business-related query, analyzes it, and provides an accurate answer in just 15 minutes. Running relevant searches for the data required in the query, the platform studies the current customer social behavior and models a prediction of the future behavior.

Based on this extrapolation, the platform authors an answer to the requested query. The app is said to be 'Inventing Google for predictive analysis' and has the potential to replace data scientists in the future.

What we now see is just the tip of the big data iceberg. There are many more applications that are employing the technology to simplify or improve the current methods and standards. The technology is expanding its limits and is being made available for most of the industries and sectors. But, there is still a long way to go for big data to completely assimilate into our daily lives.



Five Things you must do for your startup to succeed

India has the third largest startup base in the world, as per a report by NASSCOM. But, how many startups have lifted off the ground to become the next Facebook, Airbnb or Snapchat As the popular phrase goes?— 9 out of 10 startups fail?—and there are numerous reasons for it including slow to no funding, low product demand, and tough completion.

An entrepreneur's journey isn't easy, and to succeed in it, he/she needs to have some qualities that should come naturally. Let's take a look at them, one by one.

#1 Know your Customer

The overarching rule of successful startups? know your customer. Businesses that do not focus on customers will fail. Period!

As a successful entrepreneur, you will know who are the potential customers, how to reach out to them and plan strategies to retain them. Moreover, understanding your target customers gives you an advantage of solving their problems, and essentially making changes in the services/product and make it a market fit.

To achieve this, you will need to spend quality time on market research, studying changing patterns of consumer behaviours, buying habits, and the market size. Further research/analysis on factors

such as gender, region/area, age groups and interests of your customers is also important. Customer satisfaction surveys are a great way to know how consumers responded to your products and services.

Measuring customer satisfaction helps bring valuable insights. For instance, it helps with customer onboarding i.e. introducing new customers. However, always remember, customer retention is cheaper than acquiring new customers. Proactive support, customer follow-ups, frequent assessments and personalized experiences help customers have a positive experience. New customers can be gained via recommendation from the older ones.

#2 Stay Updated

"It is not the strongest or the most intelligent who will survive but those who can best manage change." ?

- Leon C. Megginson

In the fast changing ecosystem, companies need to evolve and adapt quickly to the consumer needs. Companies that do not adapt will fail. We've seen powerful ones like Nokia, Blackberry and Kodak wither away, nothing could save them, not even their large base of loyal consumers.

For instance, Kodak, a 124-year-old manufacturer who ruled the photography world for decades had to file for bankruptcy in 2012. Its customer base soon moved

ahead and away from the traditional films and cameras towards the digital era.

For startups, innovation is even more important. A study by IBM highlights that 90% of Indian startups fail within the first five years due to lack of innovation. Consumers are fickle-minded, so it is important for you to understand how customers perceive and interact with the industry and anticipate their expectations for the future. So, pay attention to trends, stay updated with the latest technologies, keep an eye on competition and do not indulge in too much procrastination.

#3 Impose self-discipline

"If you do not conquer self, you will be conquered by self."?

- Napoleon Hill

Self-discipline is the foundation of success and something you must follow and impose. In the current digital age, you need to excel physically, mentally and emotionally. This can be done through discipline. It's the ability to continuously accomplish tasks by doing what you have to do without getting deterred by your emotional state.

For instance, while working for yourself, it is important to stick to the working hours and not push tasks to the next day. A person can really stand out in the crowd just by being punctual and committing to deadlines. On the other hand, it is quite easy to get stuck in the cycle of delays. So, do not

underestimate tardiness. Similarly, it is important to identify and retain individuals who respect disciplined collaboration. They can be valuable assets and will work towards your goal of making your startup successful. It helps you decide ahead of task, manage budget without going overboard, force yourself to stick to the schedule, achieve goals, and have a good work-life balance.

4 Manage budget

Whether bootstrapped or funded, we don't need to emphasise on what an important role budget plays in building a startup. It ensures that your business has a future. But, it is also important to control the cashflow and plan your budget prudently. Some common mistakes are assuming a large funding can suffice and cover all expenses. No! Planned budgeting and controlled expenditure can ensure that.

Do not get caught in a debt trap. It is often seen that a business can flourish while accruing debt, but the tables are turned as soon as you have to start repaying off the debt. In a nutshell, track your expenses and avoid overspending.

So, get good at budgeting or at least take help of someone who is. A set budget will help you focus better.

#5 Network and connect with the right mentors

Always remember, there is no one-size-fits-all process. One has to keep adapting to changes and will often face many first-time scenarios. This is when a mentor comes to the rescue, typically someone who has been in a similar position and waded through many successes and failures in his or her entrepreneurial journey.

The mentor may not give a perfect solution to your problem, but help you think differently to solve the same problem. A mentor will honestly evaluate your idea and also help you deal with your successes and failures on a personal level.

Moreover, mentors can assist you to reach out to others who may play a significant role in your journey. Arguably, professional networking is becoming a crucial part of business development. Networking can help you meet investors, expand your team, get brand exposure and most importantly discover new clients and opportunities, and new influencers.

Your grit and hard work will take you places, but being surrounded by the right people will be instrumental to build a sustainable business model.

Trend Micro Research Finds Major Lack of IoT Security Awareness



“A common theme in cyberattacks today is that many are driven by a lack of security awareness, and this is accentuated with IoT (Internet of Things) security.”

Only 14% of respondents say they have complete organizational awareness of IoT (Internet of Things) threats

- 37% claimed they are not always able to define their security needs before implementing IoT solutions

- 59% of corporate IoT attacks target office devices

Trend Micro Incorporated, a global leader in cybersecurity solutions, recently revealed that 86 percent of surveyed IT and security decision makers across the globe believe their organization needs to improve its awareness of IoT threats. This significant lack of knowledge accompanies rising threat levels and security challenges related to connected devices, which leaves organizations at great risk.

The poll of 1,150 IT and security leaders reveals a worrying lack of cybersecurity maturity in many organizations around the world as they deploy IoT projects to drive innovation, agility and digital transformation.

“A common theme in cyberattacks today is that many are driven by a lack of security awareness, and this is accentuated with IoT security,” said Kevin Simzer, chief operating officer for Trend Micro.

“It’s a good first step to see that IT leaders recognize awareness levels need to rise across the organization. We recommend business leaders clearly acknowledge the IoT security challenges affecting their company, understand where their security requirements, and invest accordingly to make their security goals a reality.”

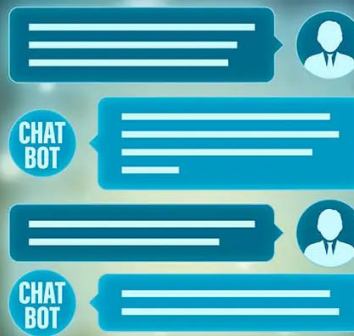
A lack of IoT security awareness leaves companies increasingly exposed to potentially damaging cyberattacks. According to the survey, current attacks are targeting office devices most, followed by manufacturing and the supply chain. When an attacker compromises these devices, they can also gain access to the greater corporate network to conduct even more damaging attacks.

To protect against IoT security attacks, more than 50 percent of surveyed IT and security decision makers reported they prioritize a few key capabilities in their security solutions.

Monitoring for anomalous behaviors and vulnerability management were the most sought after requirements to mitigate the risk of IoT devices being compromised.

In addition to these specific capabilities, Trend Micro recommends a strong network defense approach to ensure IoT devices do not add security risk at any part of a corporate network. The company also offers a range of security solutions related to specific types of IoT devices for additional protection.

Three sad truths about chatbots that will leave you shocked..!



by Naveen Joshi
Founder & CEO - Allerin, Mumbai

✍ Chatbots pioneer a new way for organizations to connect with their customers. But, the truth about chatbots is, they still lack the potential to gauge human emotions and deal with complex queries.

Organizations have now understood that humans get more attracted towards only those companies that provide assistance in lesser time. Once such technological innovation, that offers speedy and accurate service is, chatbots. Chatbots have blown everyone's mind to a level never imagined. It is quite shocking to know that 69% of consumers would love to communicate with chatbots while interacting with brands. With such hype, organizations have started capitalizing on chatbots for their business to enhance their customer experience.

But, the truth about chatbots is they are over hyped. This incredible AI's application (currently) falls short on emotional intelligence and smartness. Let's dig more into the sad and heartbreaking truth about chatbots.

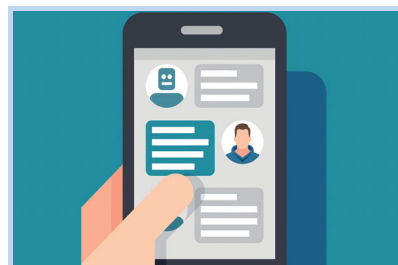
» They fail to maintain the conversational flow

We know that for a conversation to be successful, there is a need that both ends should share meaningful context. It's a collaborative approach. But, in the case of

chatbots, it sometimes isn't what we get. Chatbots, in most cases, fail to maintain the flow in the conversation. They lack the ability to remember the dialogues that you had with it in the past. This results in customers typing the same message again for the information they need, when they restart a conversation. This lack of context awareness for a chatbot happens because of 'not-so-advanced' NLP algorithms.

» They lack in gauging human sentiments

Chatbots are mostly used as an information acquisition tool. Chatbots can answer queries of customers efficiently for which they are being trained. But, when it comes to understanding empathy, they fall short again. Due to the lack of emotional intelligence, chatbots cannot gauge the sentiments of humans. Chatbots have a



"Chatbots, in most cases, fail to maintain the flow in the conversation. They lack the ability to remember the dialogues that you had with it in the past".

lack of comprehension on sarcasm, jokes, and humor. They might take a human joke as a frank thing, thereby providing irrelevant information to customers. If humans do not obtain the required assistance, then it won't leave a good brand impression on them.

» They can't perform more than one task efficiently

Organizations strive to develop a chatbot for dealing with every kind of business, similar to a personal assistant. But, chatbots lack improvisation skills. Let us be clear that we do not doubt the assistance provided by chatbots. They can answer accurately based on the training they obtain. But, chatbots can explain only templated queries. If you try to question chatbots again and again, it overwhelms them, leaving them confused. For clarification, they will keep on asking the same question to customers, leaving a bad impact altogether. The customer might get annoyed with such a negative experience.

Honestly, chatbots are one of the most promising application areas of AI, aimed at transforming the organization's services and customer's experience. For now, there are several flaws (which will not last for long, for sure) due to the immaturity of its parent technology. Chatbots, as they evolve, can give an inclusive solution for your business, easing the life of your users. As of now, by knowing the truth about chatbots, you can decide appropriately whether they are worth an investment for your business or not.

Staying Safe on Social Media



✍️ The family meeting now involves discussions on Internet safety for kids — what parents expect from their children in terms of responsible Internet usage, and discussions about common-sense precautions that will keep kids safe online.

Social media is of particular importance here. According to a recent Pew Research Center Internet report, 81 percent of teens surveyed between the ages of 12-17 use social media, and while many kids have profiles on common sites like Facebook, they aren't always active on those sites for a variety of reasons: Some kids feel pressured by too much sharing, perceived or real bullying or because they don't feel free to express themselves. They may then gravitate towards newer social sites that parents are not aware of. Parents need to know where their kids are online, who they are interacting with, and just as importantly, why they prefer certain social sites over others.

» Social Profiles and Privacy Settings

Every social site begins with creating a profile. Kids are getting more savvy about what they put into a profile, but it remains the parent's job to review it, as it is a key point regarding online safety for your kids. In terms of a profile, less is more. Nobody online needs to know where a child goes to school, relationship status, names of pets past or present, home or email addresses, phone numbers or any other identifying information.

Parents can coach their kids about how nefarious individuals use identifying information to gain access to personal accounts, to spam, impersonate them or otherwise cause harm. Help them set their privacy settings to strictly limit who can see their social media activities and view their profile. Friends of friends, for example, don't need to see their posts and photos. Periodically review their privacy settings to ensure that nothing has changed.

» The Hazards of Over-Sharing

The same is true regarding "over-sharing." It may be seemingly innocuous to post details about being home alone, but such information could put a child at risk. The same is true about telling online friends about vacations, which is essentially telling the world when your home will be unoccupied. Kids may not understand that a simple post asking for a phone number may be from a malevolent source. Parents can help by discussing various scenarios with their kids, so that they understand what kinds of information should not be shared via social media.

» What Goes Online, Stays Online

Children often get drawn into peer drama, blowing up the social media sphere with arguments and snarky commentary. Bully behavior may crop up, leaving kids feeling vulnerable and alone. Kids may be quick to take a video and post it online without thinking through the consequences. Parents can do a lot to explain that what goes online, stays online. Forever. Teach kids to take a breath before posting, and to never immediately take to Facebook or Twitter in the heat of anger. Parents should be firm that comments, actions and online behavior should be governed with the same courtesy and respect as kids would convey with people they meet face-to-face.

» Mobile Safety and Social Media

Internet safety for kids includes mobile. More children have access to the Internet from their phones, tablets and handheld gadgets than ever before. Mobile access also means that kids have the ability to very quickly move to new social media sites before you'll ever see the evidence on the family computer. Setting firm rules about joining new sites is key, as is keeping communication open. Ask why your child may feel the need to jump into a new social media site, whether it is to get away from bullying behavior or simply to be a part of a newer, kinder, gentler online community.

» Top Job for Parents ...

Internet safety for kids seems like a daunting task in the face of the ubiquity social media, but it's certainly necessary and important. Model for your kids the online behavior you expect of them and insist upon friending and following them on their social sites. Set up parental controls and be sure to stay on top of new social sites and determine if they are appropriate for your kids. Because mobile access increases your child's overall exposure to social media, it may be helpful to invest in mobile security software with parental control tools to help monitor your child's mobile activity. Above all, make Internet safety a top family priority.

"Some kids feel pressured by too much sharing, perceived or real bullying or because they don't feel free to express themselves. They may then gravitate towards newer social sites that parents are not aware of. Parents need to know where their kids are online, who they are interacting with, and just as importantly, why they prefer certain social sites over others".

How to Generate Strong Passwords for Your Social Media Accounts



✍ When you think of social media, you probably think of sharing links and messages with trusted friends. In reality, however, social networks often are a haven for hackers. Because many users let their guard down when using social websites, exploitation schemes have been spreading all over social media sites — making it difficult for users to avoid malware and scams. Fortunately, you can protect your digital identity by using a strong password generator, a solid security suite and plain common sense.

» Threats from Social Sites

It's crucial to exercise care when browsing social sites, because it is often tough to tell whether something is legitimate or not. For example, just because a friend posts a link or installs an application, that doesn't mean the content is safe to visit. After installation, many malicious Facebook applications will post spam links without the user's knowledge. Some websites even trick users into adding malicious applications to their accounts without warning.

Another common tactic of scammers is to hack into user accounts and then send IMs and private messages to the users' friends. The attacker poses as the friend, saying he or she has been mugged while traveling, and needs money wired immediately in order to get back home.

In reality, the friend usually is unaware of

the attack, or is locked out of his or her social media account. Typically, any requests to wire money should be met with skepticism, as that is one of the most popular ways for scammers to transfer funds.

» Secure Your Online Accounts

As a rule of thumb, you never should use the same password on more than one website, because when hackers steal social-media passwords, they will try those credentials out on banking websites as well. Although the sheer number of websites on the Internet has made it nearly impossible to memorize all your unique passwords, by using a strong password generator you can create unique credentials for every website you visit. These credentials are then stored in an encrypted digital database, which makes your information indecipherable until you log into the password manager.

One of the biggest benefits of using a password manager with an integrated strong password generator is that through the auto-login feature, the software will automatically fill your information and credentials into login and registration forms without user intervention. Additionally, by using a virtual keyboard to enter sensitive information, users are able to avoid malware that tracks key strokes. The final major feature of password managers is that they often allow you to run a portable

"Common tactic of scammers is to hack into user accounts and then send IMs and private messages to the users' friends. The attacker poses as the friend, saying he or she has been mugged while traveling, and needs money wired immediately in order to get back home".

version on a flash drive so you can take your passwords with you regardless of where you are.

» Ensure All Your Devices Are Protected

Chances are good that you access your social-media accounts on multiple devices. Whether it is a tablet, laptop, smartphone or any other type of computer, it is vital to ensure that the devices you use are fully protected from digital threats. For full multi-device security, it is crucial to not only run a security suite on your computer, but also to have a reputable anti-malware package on your smartphone. This ensures that no matter where you use the Internet from, you are always using a clean machine.

While there are many security suites on the market, you can download free antivirus trials to test the various packages and choose the right one for you. Ideally you should choose a suite that offers comprehensive protection (i.e. anti-malware, anti-spam, firewall, etc.) because having all your security solutions from one reputable vendor is preferable to using a hodgepodge of software.

World Class GAMING STORE Now in Hyderabad



All Gaming Consoles, Games CD'S ,Accessories (Sale's & Service's). PS4 PRO, PS4 SLIM,PS4, XBOX ONE X XBOXONE S, PS3, XBOX 360, PS2,PS VITA, PSP ETC..



Published & Distributed by

**World of Multimedia
COMPRINT**

1st Floor, Pavani Kamal, Opp. SBH Gunfoundry,
Abids, Hyderabad. Ph - 040 66629647/48
e-mail : comprint@gmail.com
9248018430/31/34/36

For Demo Visit Us:



Watch on youtube.com/comprintmultimedia



Be our fan on facebook.com/comprintcdworld



Be our fan on twitter.com/comprint



www.comprintcdworld.com



9154733845

*Conditions Apply

WHERE YOU LEARN IS AS IMPORTANT AS WHAT YOU LEARN.



Dilsukhnagar Arena is the No.1 Centre of Arena Animation in India and the largest Training facility for **WEB, GRAPHICS, ANIMATION** and **VFX** in the country.

We ensure truly global standard facilities, world-class labs with Production-class technologies and finally the best placements. So, why join elsewhere?



© Creative Multimedia

Enhancing Employability™ of creative talent. Since 1998

📍 Arena Animation, Sai Towers, Main Road,
Dilsukhnagar, Hyderabad - 500036, Telangana.

📞 +91 801 901 3388
+91 801 901 3399

✉ enquiry@bestmultimedia.com

www.BestMultimedia.com

Extensive Industry Tie-ups | Regular Campus Drives | Revolutionary Initiatives | Multiple Value Additions