VIDYAVARDHINI'S COLLEGE OF ENGINEERING AND TECHNOLOGY

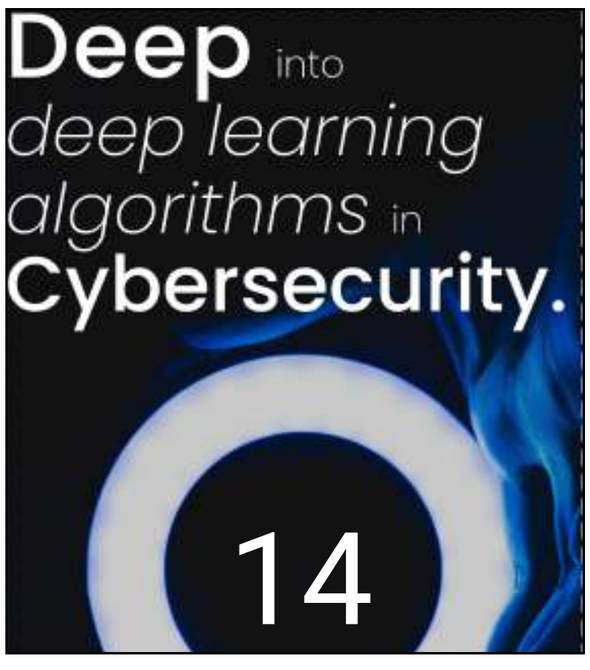
DEPARTMENT OF ELECTRONICS AND TELECOMMUNICATION ENGINEERING

ETA *PULSE*

11th EDITION | MAY 2021

CYBER *SECURITY*

Zero Trust 8



11 My Data is **NOT FOR SALE!**

Contents

From The HoD

Over the years, the ETA committee has journeyed a long way to fulfilling **"Knowledge is Power"**, it's core mission. It works not only towards the technical skill development of the students but also towards developing their soft skills by teaching students the importance of team work along with all the skills required to design and develop a magazine from scratch. It is quite gratifying to see that ETA has come up with its eleventh edition of Pulse magazine i.e. *PULSE'21*. This year, PULSE explores the up-and-coming and ever improving field of *CYBER SECURITY*. The magazine also additional insights in the form of alumni interviews, departmental activities and much more.

Though it has been such a tough year due to the Global crisis, we put forward our best efforts to shine bright with excellent exam results as well as placement in various reputed companies like Infosys, TCS, LTI, Zeus Learning and many more. Apart from this, IEEE & IETE students' chapter organized various seminars and workshops for students and teachers to acquire knowledge beyond their realm of the academic syllabus. All this wouldn't have been possible without the spirit of co-operation and understanding between the staff and the students. I would like to appreciate the efforts of Mrs. Ashwini Katkar, the staff in-charge of ETA for doing such a great job. I convey my warm regards to the entire ETA team for their relentless efforts and extend my best wishes for their future endeavors.

-Dr. Vikas Gupta

From The Staff Incharge

“Be ready to change your Goals, but never change your values”!
-Dalai Lama

It is with great pleasure and pride that I present to you our magazine, ‘*Pulse’21*’!
Covid-19 has affected everyone’s life more or less, but since life never stops for anyone, various ways were conceived to increase productivity even in this restricted times. And all of us accepted the new trend of ‘**Online is the New Normal**’.
This entire huge data communication on internet, instigated drastic traffic load on the Telecom Networks and data privacy and security became most significant. Considering all this in mind, we present our eleventh edition of PULSE Magazine “*Cyber Security*” organized well by articles about firewalls, Deep Learning advancements in cybersecurity, its application in different fields and scope. The magazine also includes Motivational section - Alumni Talk and Student Achievements.
Continuing the trend this year too, ETA published informative and rich newsletters. This year we decided to modernize the overall design of the magazine to make it more in-line with today’s design trends whilst also providing a great reading experience as the magazine is filled with rich detailed interesting topics.
I am delighted to witness the progress of students in co-curricular and extracurricular activities, and I’m sure the excellent team building skills that they learn whilst working here is going to help them further down the line. I devote my sincere gratitude to our Principal **Dr. Harish Vankudre** for his valuable support and our HOD, EXTC and Dean Academics **Dr Vikas Gupta** for his immense guidance and support. I would like to appreciate the work done by our Secretary, **Mr Nihal Kumar** and his entire team. I would like to appreciate the whole ‘ETA team’ for their valuable efforts.

-Prof. Ashwini Katkar

From The Secretary

Great achievements are a result of slow incremental developments, something that may have been learnt over a span of several years. We often consider such tiny incremental developments as trivial, but widening your horizons not only opens up your opportunities but they end up giving you new perspective on things. That's why taking that leap to try something new is essential. This was the mindset that I had when I decided to become a member of ETA and looking back, I'm glad I made that decision.

This year we decided to modernize the design of the magazine, to bring it in-line with the current design trends. Not only did we all learn about these design trends but it also introduced us to fields like UI designing and Information Architecture, which the members could further delve into and maybe even pursue as a career.

The one thing that I wanted to achieve during my time as the secretary was to make sure the team develops a skill or two, something they didn't posses before joining, and I think I have succeeded in that regard. I hope the next person to lead the team follows this tradition of bringing something new to the table and focusses on overall development of the team along with the periodical literature.

I would like to offer my sincere gratitude to our respected HOD, **Dr. Vikas Gupta** and our Staff-incharge **Prof. Ashwini Katkar** for their valuable support and guidance. I would also like to thank my team, without them this magazine wouldn't have been possible.

-Nihal Kumar

Cyber Security

The disaster you can't see but can be prepared for.

Cyber security consists of the policies, processes and practices adopted to stop , detect and monitor unauthorized access, misuse, modification, or denial of a network and network-accessible resources.It also involves the permission of access to data during a network. it's then controlled by the network administrator. Then, the users pick or are assigned an ID and password. they will even be given other authenticating information that permits them access to information and programs within their authority as assigned. Cyber security generally covers a spread of computer networks. It includes both public and personal networks, that are utilized in chores. They're used for conducting transactions and communications among businesses including government agencies and individuals. But, one must note that, Networks are often private. For e.g. : within a firm, et al. which could be hospitable public access. Cyber security is involved in administrations, enterprises, and other sorts of establishments. It does as its name says: it secures the network, also as protects and oversees the operations which are being done. the foremost common and straightforward way of protecting a network resource is to assign it a singular name and a corresponding password.

Cyber security consists of hardware and software tools and are ideally composed of stratums that include applications, antivirus, access management, servers, firewalls, physical access, and policies.

Cyber security vulnerability refers to the possible insecure points within the network which will be abused by an invader for unapproved access. Vulnerabilities allow attackers to snoop, access a system, install malware, and steal, destroy, or alter sensitive data.

Cyber security covers many technologies, devices, and processes. It always refers to a group of rules and arrangements designed to guard the integrity, confidentiality, and accessibility of computer networks and data.

Terminologies:

Vulnerability -
A vulnerability may be a element that leaves a system hospitable misuse (e.g. a network cable or a protocol weakness).Vulnerabilities allow attackers to spy, access a system, install malware, and steal, destroy, or modify sensitive data.

Threat -
A threat indicates the potential for a violation of security. A network security threat is an attempt to get illegitimate admittance to your organization's network, to require your data without your knowledge, or implement other malicious pursuits.

Attack -
The term attack is applied to an attempted violation. Network security attacks are unauthorized actions against private, corporate or governmental IT assets so as to destroy them, modify them or steal sensitive data.

Firewall -
A firewall is software or firmware that forestalls unsanctioned traffic from accessing the network. Firewalls provide a group of rules about which data packages can come and go from the network to subordinate the danger of harmful packets or network security threats.

Microsegmentation -
Network security specialists use microsegmentation to fragment a network into smaller pieces or segments to simplify overall security running of the network, even in cloud environments or data centers. Micro-segmentation helps enable IT to deploy flexible security policies deep inside a data center using network virtualization technology instead of installing multiple physical firewalls.

VPN-
A virtual private network uses encrypted connections to attach approved users to a network and its resources. VPNs are commonly available in two forms: remote access VPNs and site-to-site VPNs. Remote access VPNs use IPsec or Secure Sockets Layer to firmly enable remote users to send and receive data as if they were directly connected to the network. The VPN software runs on individual, remote devices and permits individual remote employees safe access to their organization's main network.

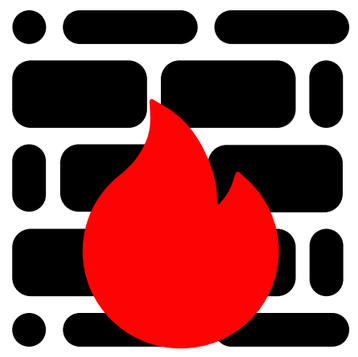
Zero-trust network -
All traffic endeavoring to access a zero-trust network must endure strict identity and device verification albeit the traffic source is inside the network. Zero-trust networks provide users with the smallest amount amount of access possible and use micro segmentation to segment the network.

Network access control -
NAC limits user and endpoint access to network resources so as to strengthen security. NAC systems legalize permitted user actions and are ideal for networks which will strongly control user environments.

Blockchain -
Blockchain may be a system that records data transactions within a peer-to-peer network -- where each node functions as both client and server. Each node can access the record to avoid one point of failure, which may benefit establishments with network appliances from different vendors and organizations that cope networks through a centralized controller. Although blockchain won't be a standard network security technology, it shows potential to trace and secure formation changes and records.

References: *https://www.eccouncil.org/network-security/*

Better **Safe**
than **Sorry**



Why are firewalls necessary?

Not the wall Trump wanted to build

The term "firewall" originally referred to a concrete wall that could prevent a fire from spreading inside a building, or a car, to buy more time for passengers to escape. The software or firewall firewall you may have on your PC or network, works the same way. Like a wall, it is designed to prevent “fire” (in this case, cyber threats) from entering.

With an active firewall you can block unauthorized access to your computer and network. This protects your data from being compromised. It also gives you extra protection against viruses and malware. If a firewall detects any suspicious or malicious attempts to install your private network from the Internet, it will not let you pass.

At home, you may have a software-based firewall, but your business will need a Hardware-based firewall to keep all unwanted traffic out of your network. A business-level firewall will give you the ability to control which computers in your network are exporting. Therefore, you can decide what kind of emails are sent from your network, which means you can prevent employees from sending private or sensitive information.

Why do you need a firewall?

An effective, managed firewall will greatly reduce the risk to your business. Without a firewall, your business could easily be harmed by a cyber-attack, causing you to lose all your important information. This will not only disrupt business processes, it will also reduce productivity and damage your reputation and product. Cyber criminals can easily scan every computer connected to the Internet and try to infilterate their programs. Without a firewall, they can access your important files, install, delete or misuse them. The potential consequences of this can be catastrophic, often leading to significant financial losses, damage to dignity, and penalties from the authorities.

But a well-designed, and well-maintained firewall will protect your data, network, and devices. Most importantly, you need to make sure your firewall has the ability to manage normal and encrypted internet traffic without delaying your devices or endangering security.

If you have a good IT support partner, they will set up and manage your firewall and take care of all security updates. Thus, you can be sure that your firewall is maintained by a team of IT professionals, helping to protect your business from new and emerging threats.

How can an active firewall protect you?

1. Remote login

Remote login refers to any method of controlling a computer from a remote location. Malicious actors are constantly developing more and more creative ways to access private data and secure information that they can use as leverage for ransom payments.Cyber criminals have the tools to login to your devices remotely. They can then control the device, steal information, or install malicious programs and spyware. An active firewall will help prevent unauthorized access to

The term “firewall” originally meant **a wall that was created to confine a fire** or a potential fire in a building to keep it from spreading.

your devices via the Internet.

2. Email session hijacking
If cyber criminals gain unauthorized access to your network, they may hijack your SMTP server. This means they can send spam or malicious emails to your contacts via your email. This can seriously damage your reputation, causing clients to lose confidence in your product and their safety. An active firewall helps protect against hijackings by email, ensuring that the important relationships you have with customers are maintained.

3. Application and operating system backdoor vulnerabilities
A backdoor is a malware type that negates normal authentication procedures to access a system. As a result, remote access is granted to resources within an application, such as databases and file servers, giving perpetrators the ability to remotely issue system commands and update malware. Certain programs and applications can give cyber criminals remote access to your network by features or bugs, empower them over the system and put your employees and data at risk. A firewall will help block hidden access and ensure your apps are secure.

4. Denial of service
Denial of service is an invasive, disruptive attack on your server. In this case, your server will receive a connection request. When the server tries to respond, it cannot detect the system that requested it. If your server is frequently attacked by these types of connections, it may slow down and cause them to crash, which means that your productivity is disrupted. An effective firewall will prevent this type of attack from happening, ensuring that your server is not compromised by disingenuous requests.

5. Email bombs
Similar to denial of service attack, an email bomb sends the same message to a server address so many times that it causes the server to crash. Again, an active firewall will prevent these attacks and ensure that your team can continue to operate without interruption.

6. Malicious macros
A macro is a rule or pattern that determines how an app will work. Cyber criminals can create macros that tell your apps to do things you don't want, such as deleting data or hitting a computer. An active firewall will prevent this attack, keep your data safe and productivity enhanced.

7. Virus
Viruses are very common and can cause great disruption to businesses. In fact, the global cost of malware (including all viruses) has risen from £ 366 billion in 2015 to £ 1.5 trillion in 2019, which is projected to reach £ 4.4 trillion by 2021. and emails. Viruses specifically can spread extremely quickly through networks and emails, often carrying out unwanted activity. For example, viruses can monitor your activity, slow down your device, delete or lock data, and even infect your device. An active firewall will block viruses before they enter your network, protecting your devices from being infected with malicious software.

“Build a Wall”

Firewalls are one of the security measures that protect a system from hackers and cybercriminals that are active over the Internet, hacking and tampering with the functionalities of a system.

References:
https://www.netstar.co.uk/why-do-i-need-a-firewall-business/
Attribution: *Cover art by Nihal Kumar*
Artwork by slidesgo at Freepik

Did you know? **60% of small businesses shut down** within six months of a cyber attack

Optimization of cost over tools

A better solution?

Are you trying to optimize your existing tools and apps to squeeze more out of them while higher impact digital initiatives fall farther away from reach?

While the cloud offers significant benefits, its inherent elasticity and scalability tend to give rise to uncontrolled cloud costs. Cloud costs can be opaque and difficult to analyze; without some system of identifying the source of costs and managing them, they can quickly undermine your profit margin. Network optimization is a set of best practices used to improve network performance. A variety of tools and techniques can be used to monitor and improve network performance such as: global load balancing, minimize latency, packet loss monitoring and bandwidth management

With advancements in cloud computing services, applications are now being delivered over the public internet, as well as in private data centres. For enterprises is now even more crucial to deliver secure, high-performance applications ensuring the

highest quality of service to their end users. This involves a series of network optimization tools and techniques that can help to identify issues, allowing enterprises to choose the best course of action. Cost monitoring and optimization tools are specifically designed to give you the visibility and control you need to keep your monthly cloud bills in check and reduce your management overhead.

How to measure network performance?

There are two ways of measuring network performance – passive and active. Passive measurement tools monitor applications already on the network, gathering performance data metrics.

This gives a realistic representation of real-time conditions, since it focuses on real apps. There is also no danger of network disruption, as there is no additional traffic. Active measurement tools generate data tailored to baseline performance. This does require additional traffic, so must be scheduled at appropriate times.

How to monitor network traffic?

Traffic is one of the network optimization considerations when monitoring overall performance. For example, packet loss concerns packets of data that have failed to transmit to their destination. Enterprises can measure traffic on both ends to identify missing packets.

Other metrics for measuring performance include:

• **Bandwidth** – this is the amount of data, measured in bits per second, that can be sent over a given time period.

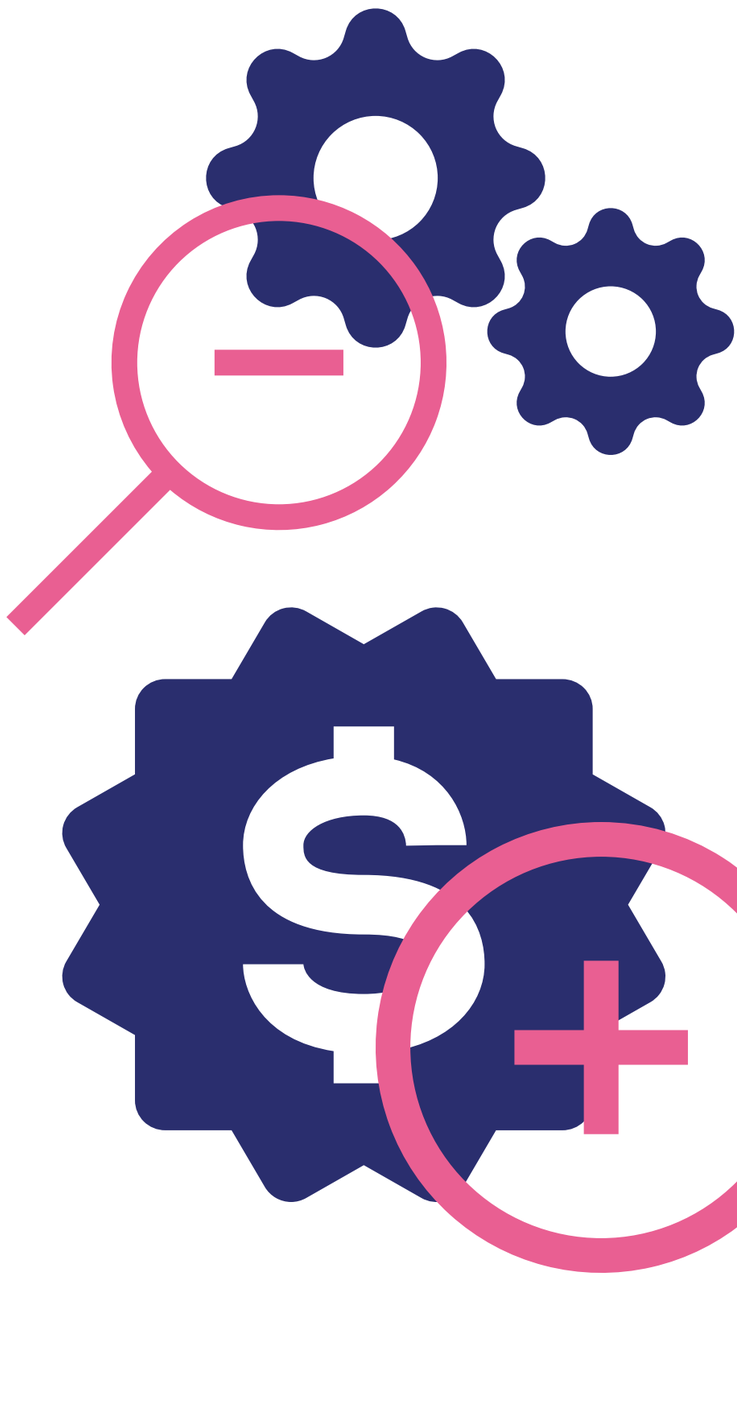
• **Jitter** – this refers to the variation in time delay for data packets sent over a network.

• **Latency** – this is the amount of time it takes for data to travel from one location to another. This is particularly important as it needs to be as close to zero as possible.

To optimize network, security and financial efficiency now you need to:

• Understand all the apps on your network and how much bandwidth they actually consume

• Eliminate duplicate packets that typically make up over 50% of network traffic



• Filter out irrelevant or low-risk network traffic that security tools don't need to inspect

• Optimize capacity of network and security tools so you are not over spending

Discover how network optimization can benefit your business.

By leveraging cloud-based network optimization and application delivery solutions, your business can:

• Reduce IT costs by offloading traffic from your origin infrastructure and by reducing demands on your Support Desk.

• Boost revenues by delivering a better web application experience for your customers and partners.

• Increase workforce productivity by reducing application downtime and accelerating application delivery to remote or mobile employees.

• Enhance visibility into application performance including end user monitoring and advanced video analytics.

References: *https://www.gigamon.com/solutions/optimize-my-network-and-security-tools.html*
Attribution: *Artwork by sunshine-91 at vecteezy*

For

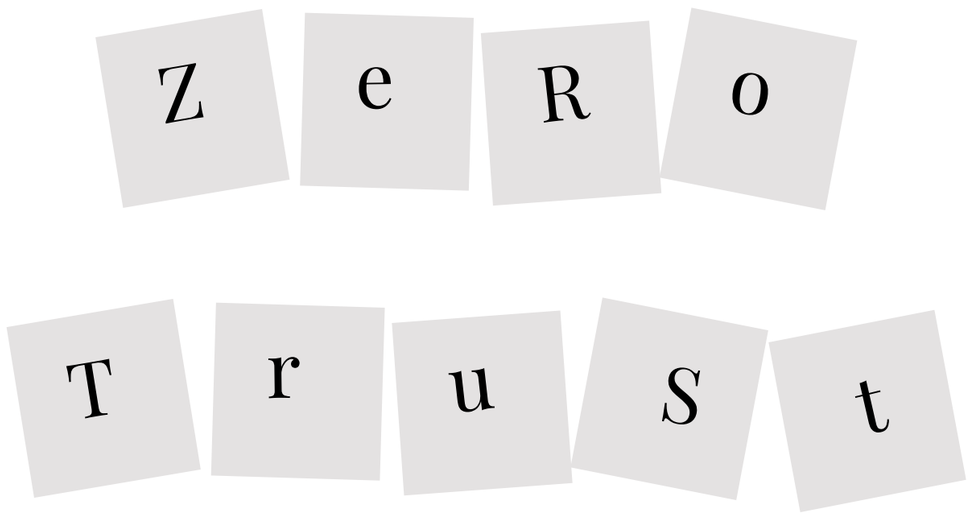
Ultimate

secure access

use

~~VPN~~

Zero Trust



Zero Trust is a strategic initiative that helps prevent successful data breaches by eliminating the concept of trust from an organization’s specification. Rooted in the principle of “never trust, always verify,” Zero Trust is meant to guard modern digital environments by leveraging network segmentation, preventing lateral movement, providing Layer 7 threat prevention, and simplifying granular user-access control.

Zero Trust Architecture

In Zero Trust, you identify a “protected surface.” The protect surface is formed from the network’s most crucial and valuable data, assets, applications and services – DAAS, for short. Protect surfaces are unique to each organization. Because it contains only what’s most critical to an organization’s operations, the protective surface is in orders of magnitude smaller than the attack surface, and is usually knowable.With your protect surface identified, you'll identify how traffic moves across the organization in relation to the protected surface. Understanding who the users are, which applications they're using and the way they're connecting is that the only thanks to determine and enforce policy that ensures secure access to your data.

Deploying Zero Trust

Achieving Zero Trust is usually perceived as costly and sophisticated . However, Zero Trust is built upon your existing architecture and doesn't require you to tear and replace existing technology. There are no Zero Trust products. There are products that work well in Zero Trust environments and people that do not . Zero Trust is also quite simple to deploy, implement and maintain employing a simple five-step methodology. This guided process helps identify where you're and where to travel next.

These Five Steps Are :

1. Identify The Protect Surface
2. Map The Transaction Flows
3. Build A Zero Trust Architecture
4. Create Zero Trust Policy
5. Monitor And Maintain

Main Principle

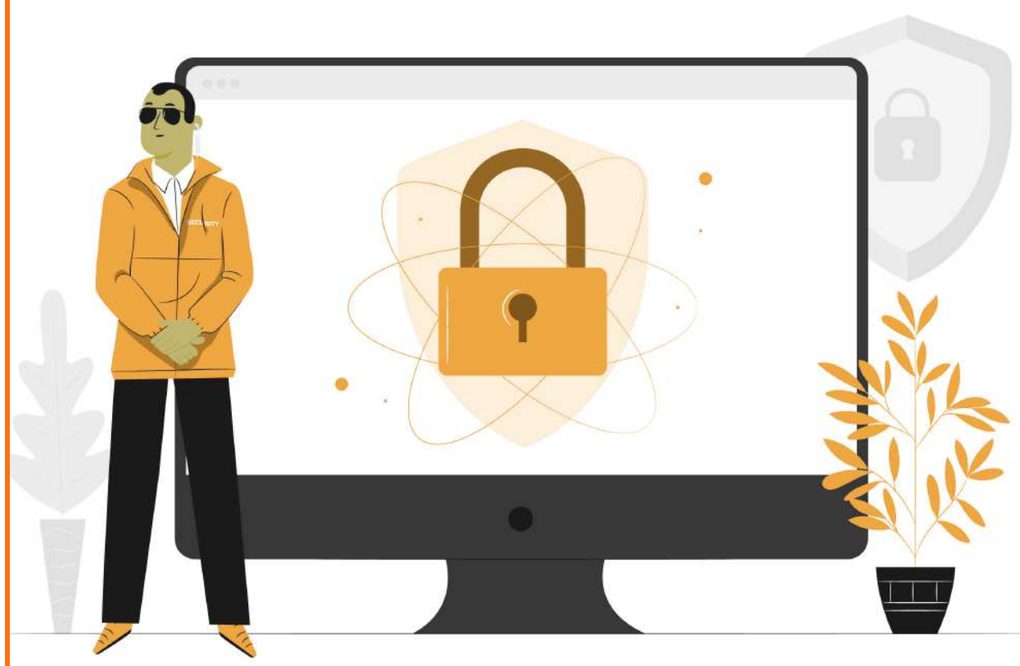
The philosophy behind the zero trust network assumes that there are attackers inside and outside the network, so no users or devices should be automatically trusted.

Another principle of zero trust security isleast-privilege access. This means giving users as much access as they need, like a general military officer giving soldiers only the required information about the mission. This reduces the exposure of each user to critical parts of the network.

Zero trust networks also uses microsegmentation. Microsegmentation is the practice of separating security perimeters into smaller areas to maintain different access to different parts of the network. For example, a network with files located in a single data center using microsegmentation may contain many different, secure locations. A person or system with access to those areas will not be able to access any other locations without special permission.

Multi-factor authentication (MFA) is also a basic security factor of zero trust. The MFA simply states that it requires more than one proof to verify the user; just entering a password is not enough to get access. The most commonly seen MFA application is 2-factor (2FA) authorization used on popular online platforms such as Facebook and Google. In addition to entering the password, users who make 2FA work with these services must also enter the code sent to another device, such as a mobile phone, thus providing two pieces of proof of identity.
In addition to the controls on user access, zero trust also requires strict controls on device access. This further reduces the area of the network attack.

Zero Trust
VS
VPN



1] Agility

• **VPN**

VPN's aren't agile. Each user or device must be found out with a VPN client and integrated into the access control system. This process is bulky and doesn't enable companies to grow with their ever-evolving business needs.

• **Zero Trust**

IT Managers and DevOps can easily add or remove security policies and user authorization based on their immediate business needs. ABAC (attribute based access control) and RBAC (role based) make life much easier when granting access to specific applications.

2] Cost Effectiveness

• **VPN**

VPN networks are CPU intensive, they create an important server load and therefore the encryptions are "heavy" as well. It takes a lot of time in maintaining the networks, adding security systems, firewalls and providing user support which are all resource intensive.

• **Zero Trust**

Easy implementation – It just needs the ZTA connector and it has a relatively simple management.

3] Usage

• **VPN**

Using VPNs for global teams faraway from the office will result in very slow and unreliable connections and also complex infrastructure and heavy costs. VPNs are also very limited when used with cloud-based applications.

• **Zero Trust**

It can be Implemented for remote work, PAMs, 3rd parties, M&As, and more.

4] Security

• **VPN**

VPN security is predicated on the castle-and-moat approach, meaning that anyone inside the perimeter can get access to the systems, assets and crown jewels. While the VPN is safer than the general public network, it's still susceptible to cyber attackers.

• **Zero Trust**

Above all, zero trust architecture provides real granular security that protects networks, externally and internally. No trust is given, so no perpetrator is allowed access.

References:
https://cyolo.io/blog/is-the-vpn-dead-vpn-vs-zero-trust/

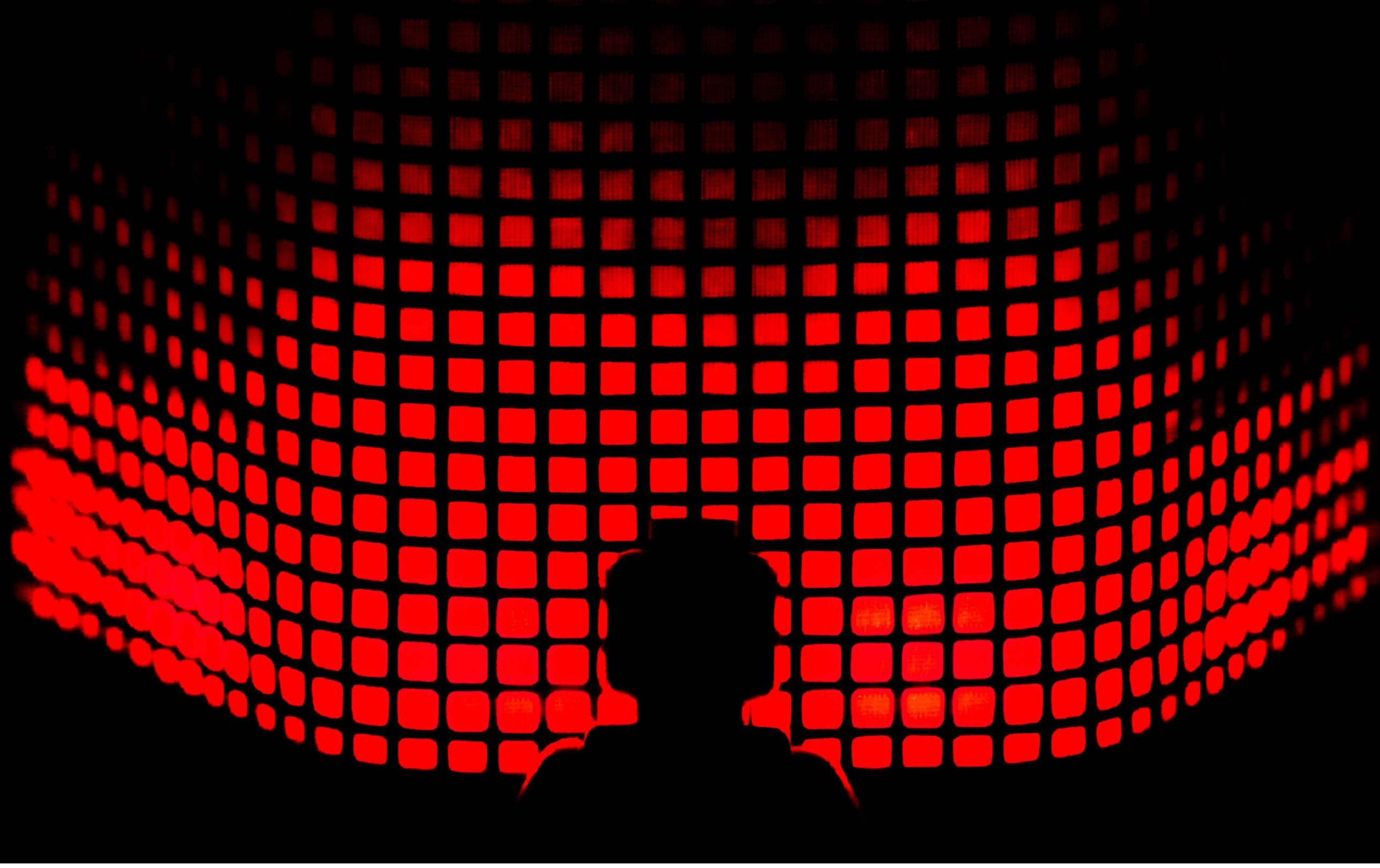
The misuse of data privacy laws

Time to act is NOW.

Social media is everywhere and every one of the time. Whether scrolling across posts on Facebook, tracking news and trends on Twitter, posting pictures on Instagram, conversing with work colleagues on LinkedIn, or making silly videos on TikTok. There are huge chances that, you and your family have a social media digital footprint. And regardless of what anyone says, everyone has some their digital footprints accessible over the web.

But all of those people online are vulnerable and tempting target for cyberattacks. Therefore the main question is how can we all stay safe while also using social media to remain in touch?

Social media users are now concerned about their privacy. These issues have spiked in recent years. Incidents of knowledge breaches have alarmed tons of users round the globe. It's forced them to rethink their relationships with social media and therefore the



A Hacking Attack Occurs Every 39 Seconds

Computers analyzed in a University of Maryland study were attacked on average 2,244 times per day. This means that a single computer could be under attack more regularly than once every minute.

security of their personal information on the web.

What are social media users worried about? Are their concerns justified? Typically, these concerns come from the large presence of social media in people's lives. 45% of the world's population uses social networks.

Threats to Privacy on Social Media:

Data Mining:
Everyone leaves a knowledge trail behind on the web on everything you are doing. Whenever someone creates a replacement social media account on the online, it starts a replacement chain. They supply personal information which will include their name, birthdate, geographic location, and private interests. Additionally to the present, companies collect data on user behaviours: when, where, and the way users interact with their platform. All of this data is stored and employed by companies to enhance target advertising to their users.

Phishing Attempts:
It's one among the foremost easy and customary way for criminals to realize access to your sensitive personal information. It could often be within the sort of an email, a SMS message, or a call, a phishing attack presents itself as a message from a legitimate organization. These messages easily trick people into sharing their own sensitive data, including passwords, banking information, or MasterCard details. It's led to many scams within the past.

Malware Sharing:
Malware or malicious software is meant to realize access to computers and therefore the data they contain. Once a malware has entered into a user's computer, it are often made to steal sensitive information (spyware), extort money (ransomware), or take advantage of forced advertising (adware). Social media platforms are indeed a perfect delivery system for malware distributors. Once an account has been compromised (often by obtaining passwords through a phishing attack), cybercriminals can take over that account to distribute malware to all or any of the user's contacts.

Botnet Attacks:
Social media bots are automated accounts that make posts. They also automatically follow new people whenever a particular term is mentioned. An outsized group of bots can form a network referred to as a botnet. Bots and botnets are prevalent on social media and are wont to steal data, send spam, and launch distributed denial-of-service (DDoS) attacks that help cybercriminals gain access to people's devices and networks.

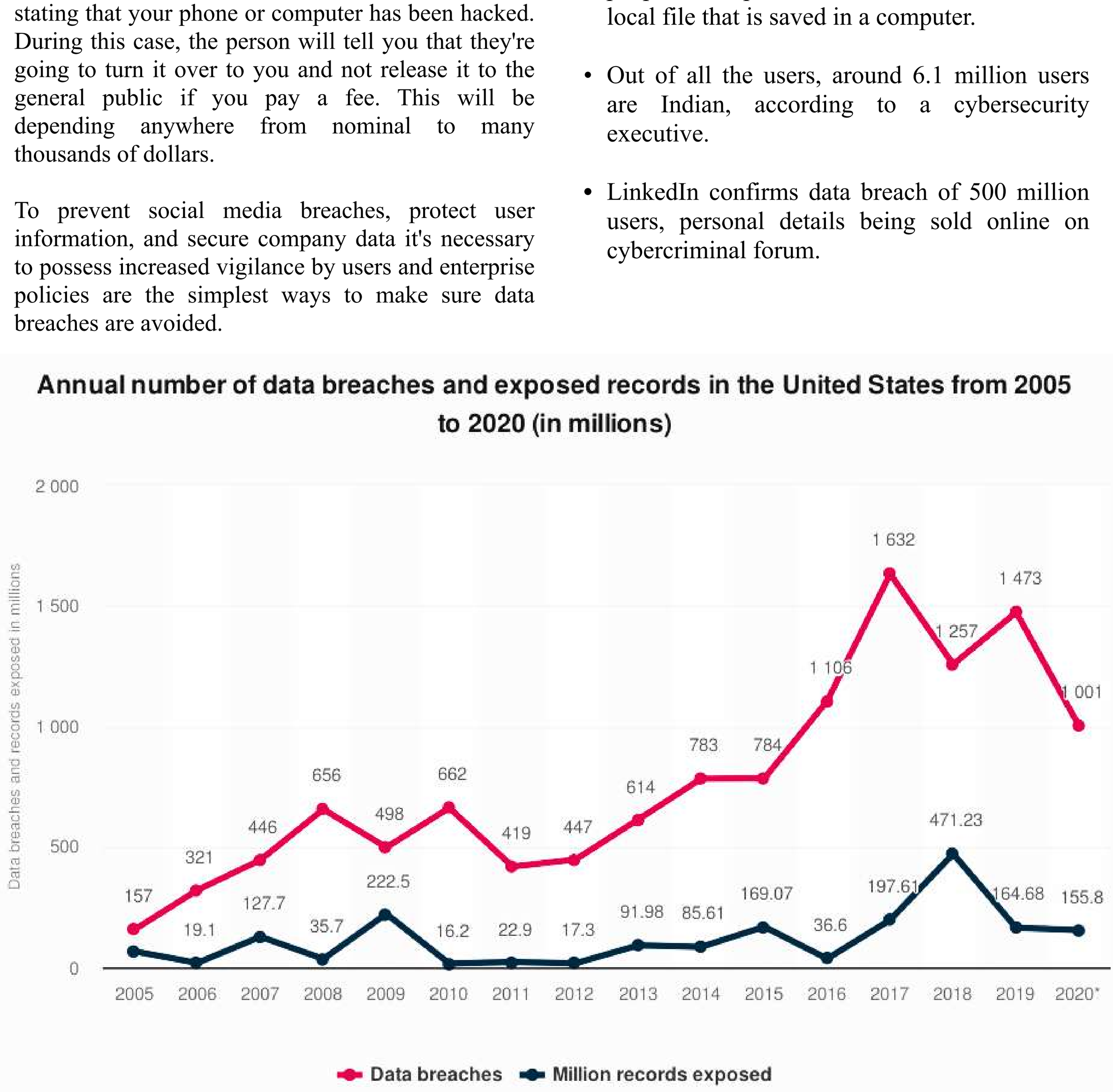
Ransomware Attacks:
Ransomware is once you suddenly get a message stating that your phone or computer has been hacked. During this case, the person will tell you that they're going to turn it over to you and not release it to the general public if you pay a fee. This will be depending anywhere from nominal to many thousands of dollars.

To prevent social media breaches, protect user information, and secure company data it's necessary to possess increased vigilance by users and enterprise policies are the simplest ways to make sure data breaches are avoided.

Recent Highlights:

- 533 million Facebook users' phone numbers and personal data leaked online.
- Out of all the users, around 6.1 million users are Indian, according to a cybersecurity executive.
- Facebook claims hackers obtained user data through data scraping — a process used by people to import data from a website onto a local file that is saved in a computer.
- Out of all the users, around 6.1 million users are Indian, according to a cybersecurity executive.
- LinkedIn confirms data breach of 500 million users, personal details being sold online on cybercriminal forum.

Annual number of data breaches and exposed records in the United States from 2005 to 2020 (in millions)



Source
Identity Theft Resource Center
© Statista 2021

Additional Information:
United States; Identity Theft Resource Center; 2005 to 2020; sensitive records exposed; excluding non-sensitive records

References:*https://sopa.tulane.edu/blog/key-social-media-privacy-issues-2020*
Attribution: *Cover art by Nihal Kumar*
Photo by visuals on Unsplash
Graph by Statista

Deep into *deep learning* *algorithms* in Cybersecurity.

Emerging Technology

What is deep learning?

Deep learning is an function of artificial intelligence (AI) that mimics the functioning of the human brain in data processing and decision-making. Deep learning is a subset of machine learning in artificial intelligence with readable networks that is capable of unsupervised learning from data that is unstructured or unlabeled. Also known as deep neural learning or a deep neural network. This has been applied towards various use cases in cyber security such as intrusion detection, malware classification, android malware detection, spam and phishing detection and binary analysis.

Deep learning has emerged in the digital age, which has brought about a burst of data by all means and in all regions of the world. This data, known simply as big data, is extracted from sources such as social media, search engines, commerce platforms, and online streaming platforms. This enormous amount of data is readily accessible and can be shared through applications like cloud computing.

How can it help in Cybersecurity?

Deep Learning is capable to solve some of our most difficult problems, and cyber security certainly falls into that category. With today's cyber attacks and the proliferation of devices, machine learning and AI can be used to "keep up with bad people," making the detection of threats more responsive than traditional software-driven methods.

At the same time, cybersecurity presents some unique challenges:

- A vast attack surface
- Tens or even hundreds of thousands of devices per organization
- Hundreds of attack vectors

A self-learning, AI-based cybersecurity management system should be able to solve many of these challenges. The technology exists to properly train the self-learning system to collect data continuously and independently across all your business information systems. That data is then analyzed and used to perform correlation of patterns across millions to billions of signals relevant to the enterprise attack surface.

Early Adopters

Google: Gmail has used machine learning techniques to filter emails since it was launched 18 years ago. Today, there are applications for machine learning in almost all of its services, which allows algorithms to perform additional independent adjustments and controls as they train and adapt.

> "Before we were in a world where the more data you had, the more problems you had. Now with deep learning, the more data the better."
>
> -Elie Bursztein, Head of anti-abuse research team at Google

Juniper Networks: The networking community is hungry for disruptive ideas to deal with today's unsustainable network economy. Juniper sees the answer to this problem as a product-ready, feasible Self-Driving Network.

Balbix: They use AI-powered observations and analysis to deliver continuous and real-time risk predictions, risk-based vulnerability management and proactive control of breaches. The platform helps make cybersecurity teams more efficient and more effective at the many jobs they must do to maintain a strong security posture – everything from keeping systems patched to preventing ransomware.

Conclusion

In recent years, AI has emerged as a necessary technology to enhance the efforts of information security teams. Since humans can no longer scale to adequately protect the dynamic enterprise attack surface, AI provides much-needed analysis and threat identification that can be done by cyber security personnel to reduce vulnerability and improve security. For security, AI can detect and mitigate risk, quickly detect any malware in the network, direct the response of events, and detect intrusion before it starts.

AI allows cybersecurity teams to form powerful human-machine partnerships that push the boundaries of our knowledge, enrich our lives, and drive cybersecurity in a way that seems greater than the sum of its parts.

References: *https://www.investopedia.com/terms/d/deep-learning.asp*

Attribution: *Cover art by Nihal Kumar*
Photo by Nadine Shaabana on Unsplash

eta social

We believe in keeping up with times. Previously, we used to update articles about technological advancements, technical events, career opportunities, and much more on the ETA wall. But, in order to increase our reach we decided to have a digital presence as well. On our instagram handle, we not only share recent highlights but also run an interview series to help motivate and guide our followers.

Come join us!

@etabyVcet

vcet.edu.in/eta-2/

Reasons to start your cybersecurity career

There are myriad reasons why a cybersecurity career could be right for you.

Cyber security is a practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. Well, with the growing prevalence of cybersecurity, it might be the right fit to get started with Cybersecurity as your career.

The need for more cybersecurity professionals becomes clear just by scanning the news: data breaches and hacking are increasingly prevalent, and businesses are recognizing the need to protect themselves from cyber-attacks. With increase in demand, it means that there's never been a better time to pursue a career in this growing field. Cybersecurity professionals are wanted in every organization due to their importance in data security. The demand for cybersecurity professionals is extremely high, and India provides a broader opportunity compared to other Asia-Pacific countries. The availability of skilled professionals who can tackle the cybersecurity issue is significantly less in India, thus opening many new doors for young Indians for a cybersecurity career. Having a university degree is a right way of starting a career in cybersecurity, but it's not the sole way. 43% of

cybersecurity professionals are certification holders, who got training besides the college degree. Having a correct training certificate in cybersecurity is a superb way of starting a cybersecurity career.

Roles as a Cybersecurity Professional

Various paths are available to attain employment as a cybersecurity professional. To begin, one must start with an entry-level job within the field and equip themselves with adequate training and knowledge for attaining different levels of progress. One can expect swift growth as a cybersecurity professional due to the increasing demand.

Irrespective of the industry, many jobs open up for cybersecurity professionals, including jobs in banking, educational, content management, and IT services.

Here are few reasons why you should consider a career in Cybersecurity.

1. Be a part of an exciting yet challenging field:

The internet touches almost each and aspects of daily life. In modern age, cybersecurity plays an essential role in ensuring online safety, as well as the safety of the essential systems that support our daily live. Well, as a cyber-security professional, you'll be working daily to keep critical infrastructure secure. It will constantly bring up facing new and engaging challenges which would in turn build your skill set.

2. Diverse & Better Job opportunities:

As cybersecurity is such a tremendously fast-growing field, there's a high employer demand for qualified professionals. Between 2007 and 2013, postings for cyber security jobs grew 74%, and consistent with the Bureau of Labour Statistics. Whereas, the employment in the field is projected to grow 18% from 2014 to 2024. It is indeed much faster than the average for all occupations. In other words, there are a lot of jobs waiting to be filled. To be honest, the demand doesn't appear to be slowing any time soon.

3. Higher Pay Packages:

The average salary in a job that requires information technology (IT) skills is 50% higher than the average private-sector job. In 2016, the median pay for a cybersecurity job was $92,600 per annum , as compared to a median annual wage of $37,040 for all workers.

4. Choice of Industry that interests candidates:

One of the foremost appealing aspects of a career in cybersecurity is that the sector are often applied to several different industries. It starts off from government to non-profit to private sector. The highest demand for cybersecurity workers are in industries that manage high volumes of consumer data, like finance, health care, and retail trade. Be any company that stores data digitally, there has to be a space for a cybersecurity engineer.

5. Build, Upgrade & use Skillsets:

Cybersecurity is a dynamic field. This attracts people from all different types of work backgrounds. This means that within the broad field of cyber security, there's a chance to differentiate yourself by drawing on your skillset from prior jobs, like information technology, administration, or accounting. At the same time, it also allows you on building new cybersecurity skills. All of those skills are often put to use in unison.

Career Opportunitites

A lucrative, growing field, cybersecurity focuses on protecting organizations from digital attacks and keeping their information and networks safe. Cybersecurity experts detect vulnerabilities, recommend software and hardware programs that can mitigate risks, and develop policies and procedures for maintaining security.

As more businesses move their operations online, and with cyberattacks on the rise, the need for skilled cybersecurity professionals is projected to grow, particularly for healthcare and financial organizations. For example, the Bureau of Labor Statistics (BLS) projects a 32% job growth rate for information security analysts between 2018-2028.

The cybersecurity field presents diverse career opportunities. Potential jobs include information security analyst, chief information security officer, security architect, and security engineer. The most popular industries that employ cybersecurity professionals include computer systems design and related services; management of companies and enterprises; credit intermediation and related activities; and management, scientific, and technical consulting services.

This guide describes the types of careers available to cybersecurity professionals, including potential salaries, job duties, and the best cities and industries to pursue cybersecurity jobs. We also explain how to prepare for a career in the cybersecurity field.

Cyber Security Jobs in India

1. Network Security Engineer

The network security engineer is a critical position within every organization. This person ensures the security systems are implemented within the organization to counter and stop threats. Their main responsibilities include maintaining systems, identifying vulnerabilities, and improving automation. They also oversee the maintenance of firewalls, routers, switches, various network monitoring tools, and VPNs (virtual private networks).

The minimum salary of a network security engineer begins at Rs 4 lakhs and can go up to 8 lakhs per annum.

2. Cyber Security Analyst

A cyber security analyst helps in planning, implementing, and upgrading security measures and controls. They continuously monitor security access and perform internal and external security audits to ensure there are no loopholes or evidence of security lapses. A cyber security analyst is also responsible for conducting vulnerability testing, risk analyses, and security assessments, and for managing the network. In addition to these tasks, the analyst trains fellow employees in security awareness and procedures, so they are aware of the best practices to be followed to avoid security breaches.

The salary of a cyber security analyst begins at Rs 6 lakhs per annum.

3. Security Architect

A security architect plays a crucial role in designing the network and computer security architecture for their company. The security architect helps in planning, researching and designing elements of security. Without a security architect, a company's security system is vulnerable to attacks. The security architect first creates a design based on the needs of the company and then works together with the programming team to build the final structure. Besides building the architecture, they also develop company policies and procedures for how their company's employees should use the security systems and decide on the punitive action in case of lapses.

The average pay of a security architect begins at Rs 17 lakhs per annum.

4. Cyber Security Manager

Cyber security managers are responsible for the maintenance of security protocols throughout the organization. They create strategies to increase network and Internet security related to different projects and manage a team of IT professionals to ensure the highest standards of data security. A cyber security manager also frequently reviews the existing security policies and ensures the policies are currently based on new threats. They also perform regular checks on all servers, switches, routers and other connected devices to make sure there are no loopholes in the security.

The average salary of a cyber security manager begins at Rs 12 lakhs per annum.

Conclusion

Those are the top five cyber security jobs in India today, but plenty of other roles exist and go unfilled, including information risk auditors, firewalls, and security device development professionals, security analysts, intrusion detection specialists, computer security incident responders, cryptologists, and vulnerability assessors.

As organizations across a wide range of different industries such as banks, government, retail, and BFSI sectors actively recruit cyber security professionals, the job demand will only go up.

References: *https://www.cyberdegrees.org/jobs/*
https://www.azureskynet.com/future-in-cyber-security/

Meet the Department

Teaching Staff

Dr. Vikas Gupta
Ph.D. (Digital VLSI Design)
Area of interest:
VLSI, Signal Processing, Digital Communication Satellite

Dr. A. Ruperee
Ph.D. (Wireless Communication)
Area of interest:
Wireless Communication

Dr. S. Jadhav
Ph.D. (Electronics)
Area of interest:
Wireless Networks

Prof. S. Khan
M.E. (Electronics)
Area of interest:
Microprocessor and Microcontroller, VLSI

Prof. S. Gosavi
M.E. (EXTC)
Area of interest:
Speech Recognition, Optical Fiber Communication

Prof. S. Supalkar
M.E. (Electronics)
Area of interest:
Image Processing, VLSI

Prof. A. Katkar
M.E. (EXTC)
Area of interest:
Computer Networks, Optical Communication

Prof. N. Gharat
M.E. (EXTC)
Area of interest:
Image Processing, Microwave

Meet the Department

Teaching Staff

Prof. E. Naik
M.E. (Digital Electronics)
Area of interest:
Neural Networks

Prof. T. Shah
M.E. (Electronics)
Area of interest:
Image Processing

Prof. M. Patil
M.Sc. (Mathematics)
Area of interest:
Applied Mathematics

Prof. Sonal Dubal
M.E. (EXTC)
Area of interest:
Microwave and Antenna Theory

Non - Teaching Staff

Mrs. Bhagyashree Rane
Lab Technician

Mrs. Diksha Save
Lab Technician

Mrs. Madhu Lade
Lab Technician

Mr. Prakash Bhobhate
Peon

Mr. Sudhir Patil
Peon

Staff Activities & Achievements

Conference/ Journal Publications:

- **Dr. Vikas Gupta** presented a paper "Enhancing Uplink/Downlink Performance of Massive MIMO System Using Time-Shifted Pilot signal Transmission with Pilot Hopping (TSPTPH)"in International Conference on Computing technologies for Automated World Transforming the (ICCTAW' 2020) at Atharva College of Engineering, Mumbai.

- **Dr. Vikas Gupta's** paper "Resolving thg Interference in 5G Millimeter Wave Through Scheduling Technique In Estimated Channel" is published in Asian Journal Of Convergence In Technology.

- **Dr. Amrita Ruperee** paper "Enhancing Uplink/Downlink Performance of Massive MIMO System Using Time-Shifted Pilot signal Transmission with Pilot Hopping (TSPTPH)" is published in Inderscience Publisher.

- **Prof. Trupti Shah** presented a paper "Stale Fruit Detection and Storing using Image Processing " in IETE international conference on global Trends in Engineering and Technology.

- **Prof. Trupti Shah** presented a paper title "Face Controlled Door Lock and Auto Attendence System" in IETE international conference on global Trends in Engineering and Technology.

- **Prof. Shaista Khanam** presented a paper title "Interfacing of TFT Display with machines" Paper presentation in 52nd Mid Term Symposium (MTS) on Emerging trends in ICT and electronics.

- **Prof. Ashwini Katkar** presented a paper title "Malware Intrusion Detection for system Security" in 52nd Mid Term Symposium (MTS) on Emerging trends in ICT and electronics organised by IETE.

- **Prof. Shaista Khanam** presented a paper title ""VHDL Implementation of pipeline processor" in 52nd Mid Term Symposium (MTS) on Emerging trends in ICT and electronics organised by IETE.

- **Prof. Ashwini Katkar's** paper "Malware Intrusion Detection For System Security" is accepted in International Conference on Communication, Information and Computing Technology, ICCICT-2021 organised by Sardar Patel Institute of Technology, Mumbai.

- **Prof. Shaista Khanam** presented a paper ""Interfacing of TFT Display with machines" in 52nd Mid Term Symposium (MTS) on Emerging trends in ICT and electronics organised by IETE

Staff Activities & Achievements

- **Dr. Amrita Ruperee**, **Dr. Sunayana Jadhav**, **Prof. Shaista Khanam**, **Prof. Ashwini Katkar**, **Prof. Neha Gharat**, **Prof. Trupti Shah** and **Prof. Ekta Naik** were part of syllabus committee for R19 C scheme of Electronics and Telecommunication Engineering, Mumbai University.

- **Prof. Shaista Khanam**, **Prof. Ashwini Katkar,** and **Prof Neha Gharat** cleared PET exam of Mumbai University.

Congratulations **Dr. Sunayana Jadhav** for Completing PhD in Wireless Sensor Networks From VJTI, Mumbai.

FDP / STTP:

- **Prof. Shaista Khanam** completed 4 weeks faculty development Coursera program -The Raspberry Pi Platform and Python programming for Raspberry pi.

- **Prof. Shraddha Gosavi** completed 4 weeks faculty development program Coursera -Introduction to Artifical Intelligence (AI)

- **Prof Ashwini Katkar** completed course "Programming for Everybody-Getting Started with Python"- University of Michigan and Coursera

- **Prof Ashwini Katkar** attended a one week AICTE Sponsored STTP on "Telecom Networks"oraganised by VIT, Mumbai

- **Prof. Shaista Khanam**, **Prof. Ashwini Katkar** and **Prof. Trupti Shah** completed 3 days TEQIP faculty development program on "Technology, Start up and IPRs" organised by Dr. Babasaheb Ambedkar Technological University, Lonere, Maharashtra

Seminars / Workshops:

- **Prof. Shaista Khanam** conducted a workshop on "Tinkercad an alternative to arduino"

- **Prof. Shaista Khanam** conducted lectures in Student development program on "Fundamentals of Embedded C with journy of Microcontrollers" under Texas Instruments innovation Lab.

- **Prof. Shaista Khanam** was part of organizing Committtee of 52nd Mid Term Symposium (MTS) organized in association with IETE mumbai centre.

- **Prof. Trupti Shah** conducted workshop on "Octave Alternative to MATLAB"

Student Achievements

- *Xzibit K.C. College*
  National Level Project Presentation Competition

Nihal Kumar
Nachiket Lele
Tarang Marolikar

- *Covideate | TechFest, IIT Bombay*
  Asia's Largest Science and Technology Festival

Rahul Kamble

- *Product Development – AY 20-21*

Sikandar Kanojia

Student Achievements

- ***Oscillations***
  National Level Paper Presentation Competition

Track 1

Kushal Raut
Riddhesh Vanjara
Varad Vartak
Karan Singh

Archit Gharat
Yash Barot
Harsh Dodiya
Amey Morye

Shubham Gaikar
Mithun Kundu
Mayank Joshi

Track 2

Anushka Joshi
Apeksha Jain

Nihal Kumar
Nachiket Lele
Tarang Marolikar

Track 3

Rahul Kamble

Sikandar Kanojia
Akhilesh Yadav

Student Achievements

- ## *Campus Placements 2021*
  *As of 12th May, 2021**

Congratulations to all placed Students!!!

Sr. no	Name	Company
1.	Sakshi Shukla	
2.	Apeksha Jain	
3.	Abdulmateen Pitodia	
4.	Anushka Joshi	
5.	Sakshi Shukla	
6.	Yash Mehta	
7.	Hemant Chaubey	
8.	Nihal Kumar	
9.	Apeksha Jain	
10.	Chintan Sanghrajka	
11.	Abdulmateen Pitodia	
12.	Kaustubh Gokhale	
13.	Jyoti Paswan	
14.	Deepak Sharma	
15.	Swarali Pawar	
16.	Mishty Sinha	
17.	Prasad Sawant	
18.	Neehal Bhonsale	
19.	Nihal Kumar	
20.	Apeksha Jain	
21.	Sharma Deepak	

🎉 Congratulations Abdulmateen Pitodia for getting placed in LTI with package of 10 LPA 🎉

Alumni Corner

Prof. Sanjeev Ghosh

Associate Professor & Deputy Head, Dept. of Electronics & Telecommunication Engg.,
Thakur College of Engineering & Technology,
Mumbai.
Qualification: B.E. (Electronics & Telecommunication Engg.), M.E. (Electronics Engg.), Pursuing Ph.D. in Technology from University of Mumbai.
Email: sanjeev.ghosh@thakureducation.org

• Please do enlighten us about your research

As part of my Ph.D. Thesis, I have carried out research to propose techniques to reduce power consumption in wireless sensors, thereby increasing he lifetime of a wireless sensor network. In the Internet of Things (IoT) paradigm, many of the objects that surround us will be on the network in one form or another. Wireless Sensor Network (WSN) technologies will rise to meet this new challenge, in which information and communication systems are invisibly embedded in the environment around us. For WSNs to deliver and live up to the expectations of a technology that is a part of the Internet of Things, it has to overcome the challenges like Energy Consumption, Fading Channels, Mobility of Nodes and Limited Bandwidth. In my research, I have proposed to use the queuing theoretic approach to develop protocols that optimize the performance of WSNs with respect to Energy Consumption in the presence of fading channels with specified compromises with respect to the other challenges.
Apart from my Ph.D. research, I have guided many projects at the post-graduate and under-graduate level. Domains of the projects I have guided are wireless communication and signal processing. I have research papers published in international journals and conferences. I have also received a minor research grant from the University of Mumbai for my project titled 'Image Processing based book reader, facial recognition along with GPS tracker for visually impaired' fin the AY 2015-16.

• Which new engineering-specialty skills have you developed during past years?

that has emerged in the last few years and drawn in attention is machine learning. I don't have to emphasize how important machine learning is for the present and future as my readers will definitely be aware that every domain of technology nowadays involves some form of machine learning or he other. I am constantly trying to learn concepts and read up on research related to machine learning. In the recent years I have also guided under-graduate projects that involve machine learning. I also plan to carry out my post-doctoral research in the area of Machine Learning.

As the demand of programming and other aspects of software grow, I have also diversified my teaching expertise. I am currently teaching Database Management Systems to my under-graduate students of Electronics & Telecommunication. I have taught Data Structures and Algorithms in the previous semester and it has been a great learning experience. I am thoroughly enjoying this new experience.

• As a professor how has your teaching experience been so far? What are your views on teaching as a profession?

I feel that no other profession is as rewarding as the teaching profession. As a teacher, one gets an opportunity to mold the minds of young students who go on to become successful entrepreneurs, technocrats etc. I believe that I have the most important role of shaping young minds and making a difference in the development of country. I have enjoyed teaching various courses and being a mentor to many of my students who happen to remain in touch after so many years. Learning new technologies and skills has helped me being relevant to the requirements of my students.

Like many other professions, teaching is a profession where one needs to constantly upgrade oneself with the latest developments in technology. I strongly disagree with the opinion that teaching is the easiest and the most laid-back profession. One cannot be a good teacher and hope to make an impact in their students' lives with a laid-back attitude. One has to be passionate about teaching like an other job, else one would not be good at their job.

• What courses would you suggest to an EXTC Student in order to improve his skills?

The future is about communication and technology that is multidisciplinary. My suggestion would be to take up MOOC/Online courses in the fields of 5G/MIMO that would help students to keep abreast of the latest technological developments in communication. Apart from communication, an EXTC engineer should also possess multidisciplinary skills like programming, databases, Big Data, and Machine Learning to name a few.

For a student to pursue research, what things should he keep in mind?

The most important requirement to pursue research is to have a research question or a problem statement. When one wants to pursue research, the most important thing one must ask is whether his/her research is beneficial to the society. Always work according to a timeline. The results of your research may not be relevant if it takes too long. Always strive to publish/present your work in reputed journals/conferences as these forums will give new ideas/directions to your work and validate the research that has been carried out.

Lastly, be original in our approach. Don't try to misrepresent someone else's work as your own.

• What's your word of advice for juniors?

My word of advice for my juniors is to always keep learning. Learning shouldn't stop with graduation. It is a lifelong process.

"I feel that no other profession is as rewarding as the teaching profession. As a teacher, one gets an **opportunity to mold the minds of young students**, I believe that I have the most important role of shaping young minds and making a difference in the development of this country."

Durvesh Pilankar

He has pursued Masters in Electrical Engineering at San Jose State University with Specialization in Computer Networks. He is currently working as a Network Automation & Tooling Engineer at Facebook.

• When you first stepped into this field, how was the vibe around? Were the people around you supportive?

I believe the vibe was very friendly and people were exceptionally supportive when I first stepped into the field. There was no crab mentality and everyone wanted to help lift each other. There were many cases where our seniors held extra lectures on how to prepare for interviews and provided study materials. People are usually supportive here if you approach them with some prior research and almost all of them are willing to provide help.

• How was your experience during the initial years? As a Network Automation Engineer what were the challenges you faced?

During the initial years, I changed about 3 jobs and worked on about 10 different technologies and coding languages related to Network Automation. I experimented a lot by being bold, understood what I really enjoyed working on and got out of my comfort zone multiple times. There were many times where I have failed during my initial years but what personally helped me was consistently analysing why I failed and minimizing the mistakes next time.
As a Network Automation Engineer at Facebook, the biggest challenge I faced was dealing with data in range of Exabyte's (*1 Exabyte = 10^6 Terabytes or 10^9 Gigabytes*). When we deal with data at such level, your network architecture and automation solutions have to be at the most optimized level and a regular brute force approach won't solve the problem

• What traits do you feel are necessary to be a successful engineer?

1. Ask!! You won't get what you want unless you ask around e.g. help from seniors, asking doubts and questions which help you improve overall, asking for projects which you really are interested in working etc.
2. Work on your strengths/things you love to do - This is the philosophy we follow at Facebook. Focussing on our strengths help we achieve really high impact which is what everyone wants in the industry.
3. Documentation - Possibly the most important trait is documenting tips and hacks which saves you hours on less useful work. Eg at my workplace, I deal with about 100 different Linux commands and coding standards every day and without any documentation, I would have to use my precious brain cells in remembering the repetitive work.

• What are some of your strengths and weaknesses?

Strengths - Coding in Python, Communication and Presentation I realized my strengths in initial years of experience. I always make sure to give about 90% of my time on working on my strengths e.g. I would choose to work on 5 different coding projects in Python, aggressively communicate with key stakeholders to identify how big of an impact it would be for the team and present it with relevant metrics once the project is completed.
Weakness - I believe one of my weakness is estimating the timelines even after being in the industry for more than 5 years. Things move really fast in the industry and especially at Facebook, thus predicting the timelines for project completion becomes tricky if you are working on 5 projects at a time.How am I becoming better at my weakness? - Take a day or two to estimate the work that needs to be done and always add a buffer time while committing to timelines.

• What has been your most challenging or rewarding academic experience so far?

I believe, Hackathons have been the most rewarding and challenging experience. Collaborating with bright minds, getting a solution within hours and working together in team is very satisfying. It is also very challenging since you have very limited time on producing a product with an actual use case. I have personally worked in a hackathon to create a cryptocurrency application where computer networking was used as a core idea for payment transactions.

• How was the academic and extracurricular activities experience when you look back now?

When I look back, all the academic and extracurricular activities made me realize how important team work is, and I personally believe it's the collaboration with my team members which has helped me become the person I am today!!

• How did the college prepare you for your career?

The college inculcated the "MOVE FAST" attitude in me eg with all the things I mentioned in my student life, there was no way that one can achieve all of it unless you react and make your decisions Fast!! It is okay to be wrong and break things while moving fast, but like a machine learning algorithm, you should adapt and keep moving.

• Your valuable suggestion for the young engineers?

1. Travel a lot and make plans on your own. It helps you to enjoy and at the same time, plan for things which are not accounted for in life.

2. Be Bold. I switched 3 jobs before I found out what I really love to do.

3. Hustle in your 20s!!

"As a Network Automation Engineer at **Facebook**, the biggest challenge I faced was dealing with data in range of Exabyte's!"

• What was student life like during the College?

Overall, it was fun and amazing and definitely not a bed of Roses!! Imagine getting up at 6am, finishing college projects, assignments, household chores, applying for jobs(an average student in a decent university applies for more than 10k jobs), interviews to get a full time job, working part time to meet your basic needs and the list goes on and on !! We travelled a lot during our vacations and explored about 30 states in the USA which I believe was the best part of College life. Also, being a student has its own perks and you get tonnes of student discounts at many amazing places.

Rajas Patil

Have an year of working experience in Embedded systems, PID controller, Sensor fusion. Previously worked on Solar panel robotic automation and Medical Ventilators in Noccarc as Embedded Firmware Engineer. He is currently working on ADAS technology in Faurecia Clarion Electronics as a Graduate Engineer Trainee (Embedded-R&D). He is also an active committee member of IEEE Young professional under Bombay Section.

• How Is Your Work Profile And Responsibilities As A Graduate Engineer Trainee At Faurecia?

It's very exciting and enthusiastic to be working on projects in Faurecia which are currently not in the market but a few years down the line, these technologies will be integrated on every single Automobile running in the future. Being in Faurecia gives me the opportunity to work on cutting edge technologies which are set to enter the market in a few years. Here I currently work on ADAS technology in embedded sensor fusion domain for various low level communication protocols. There is a lot to learn from the teammates present here and gain very valuable early experience. One more good thing about Faurecia, is they actually went through my resume and I have been put into the project where there is image processing as I had my final year project on Image processing. Thus I work on the embedded level of the image processing along with Camera and Display interfacing signals.

• What Personal Characteristics Do You Feel Are Necessary To Be A Successful Engineer?

The most important quality an Engineer must have is problem solving skill. Rather than improvising already available solutions, a good Engineer focuses more on the approach towards how an issue could be solved. This characteristic/quality gets better and better with increase in experience. Also, one must constantly get updated with new technologies in one's vertical. This is the reason, an engineer should not get satisfied with just his current knowledge, but keep updating the skill set along with the ever growing World of innovations.

What Do You Enjoy Most/Least About Engineering?

That's a great question. One should know that being a Developer/Engineer is not just simply applying the learned concepts and getting the desired output. Actual job of an Engineer is to solve the bug or issue or an unwanted behaviour in developing the system or the process. And honestly speaking, the most joyous part of solving the issue is debugging the problem. There is no joy in finding the root cause of the bug, so that further development can resume.

Talking about the least enjoyable thing is documenting all the things I do. But at the same time, documenting is the most important task of Engineer's work culture and is considered to be the best practice. The Documents could also be considered as assets of one's learning life. So yes, this is an important but not so joyous task to do.

• What Would You Suggest To An EXTC Student, What Courses Should They Consider?

As an electronics engineer there are various sectors to work in. Like one should have a good base of programming skills in C and python (automation) along with object oriented concepts to get excelled in Robotics and automation fields. If anyone is more interested to work in SOC designing and FPGA level, the person should have very good knowledge of First Year Engineering's Basic electronics and Second Year Engineering's Analog and digital electronics. The next field an E&TC engineer can get into is communication and networking. In this, one must have an understanding of various communication protocols that take place between host, receiver and so on.

So now coming back to your question, an Engineer should practically try doing stuff that he or she has learnt in the classroom. Apart from that one can take certified courses from Udemy, Coursera and other such organizations. I personally have experienced the "Fastbit Embedded brain academy's" courses on udemy are good for beginners to medium level knowledge gains. Many engineers from my field too have taken courses from Fastbit and they too recommend the same thing. Apart from this, there are various courses on communication and networking provided by CISCO and IBM

• Apart from technical skills, what others skills should students imbibe in order to be a better employee?

Just like technical skills, soft skills and communication skills to have their own importance. The first point of contact to get a job will be the talent acquisition coordinator. In the current scenario, this is possible only over audio or virtual calls. Now here your communication skills are of utmost importance. While in a professional environment, it is expected to have good communication too.

Coming to soft skills, the two most important skills one must imbibe are listening skills and the capability to work as a team. Considering myself, the volunteer work I did during my college days for various committees helped me a lot in my professional career. Volunteering during one's college days will help in working and handling things as a well-coordinated team. The subconscious mind already has experienced such tasks and now it is easy for the brain to tackle or manage such unusual situations calmly. These are the soft skills that one must possess to be always a step or two ahead of others in an organization. As I had mentioned earlier, solving or tackling these issues is the main task of an Engineer. The other equally crucial skills are like time management, good work ethics and professional email etiquettes to name a few.

• What are the most valuable lessons/skills you have learned in your work experience?

For this one, I would like to put two phrases said by one of my CDAC professors. First is "Basics remains the same". Everybody knows at what pace the technology is going on changing. The trending technology you hear today or the trending programming languages you are studying today, might not have the place in the coming future. So how can we cope up for these circumstances we are going to face in future? The answer is to get well acquainted with basics. The basic electronics, the basic hardware language and the basics of Operating systems should be well known for an EXTC engineer before entering the industry or can learn side by side when one is an entry level employee. If you are good at this, you can get easily adjusted in whatever trend or technologies arrive in the coming days.

Also, I am learning here to respect time and deadlines, which I had completely neglected during my Engineering days. One more thing to graduating students is to try getting an internship in the field you wish to pursue your career. A good internship is something of a period of 5 to 6 months with full time working. This may not be possible during college days. But to get into a core company, I have seen people doing internships after Graduating too. Which helps them to get into core electronics. Getting into core electronics is tough and requires patience along with continuous hard work. But once you get into this field, life is truly amazing and full of innovation vibes.

"Rather than improvising already available solutions, a good Engineer focuses more on the approach towards how an issue could be solved."

faurecia clarion ELECTRONICS

Krutadnyata Naik

We are extremely pleased to interview Ms. Krutadnyata Naik who is a 2016 batch pass out student from VCET. She has pursued Master's Degree in Cyber Security from REVA Academy for Corporate Excellence - RACE. She is currently working in Qualcomm, India as Senior Engineer in Automotive BSP team.

• Please enlighten us about your work and responsibilities as a Senior Engineer?

As embedded software developer, from designing the software to code writing and its testing I need to do all of that. Sometimes I need to do peer code reviews. So basically whatever are the responsibilities of Software Developer I need to perform all of them.

"One shall not stop learning in whichever field he or she is."

• How was your experience during the initial years? Did you face problems in learning the hacks of this field? (as a Senior Engineer)

I have joined as a fresher in Robert Bosch, but for our C-DAC batch even though we were fresher's we didn't get any training, as in C-DAC we have done all the embedded learnings thoroughly it was not required. So basic project related training we got. Within two weeks I landed my first project. It was a mixed experience.
Initially as everything was new for me from corporate life to working style it took me some time to get adjusted. Hacks to learn something is if you don't get anything, ask it straight away. Don't thing you may look stupid by asking this question. Not everybody knows everything. So keep asking questions :P

• What personal characteristics do you feel are necessary to be a successful engineer?

I don't consider myself as successful Engineer yet. I'm still learning and that's how it should be. One shall not stop learning in whichever field he or she is.

• How do you keep yourself Up-To-Date with Developments in your field?

I follow techies and tech news in my field on Linkedin ;). There are so many platforms available currently for programmer to code like Hacker Rank, Hacker earth, Leet code etc. I keep trying on different platform so that I don't forget whatever I have learnt at least. Recently I have started my masters in Cyber Security so currently I am working on skillset required for that.

Qualcomm

• How supportive has the college been towards your career?

Today whatever I am is because of college, mainly Dr. Harish Dixit Sir. From the start I wanted to go in the core domain, but it was not easy as mainly in our college all software companies used to come for drives. In fact that is the situation of most of the colleges. When I consulted the Harish sir, he asked me to check for C-DAC courses and that's how I ended up in C-DAC and from there I got placed in Bosch. So all thanks to Harish sir.

• Can you share any incident during you college days which is very close to your heart?

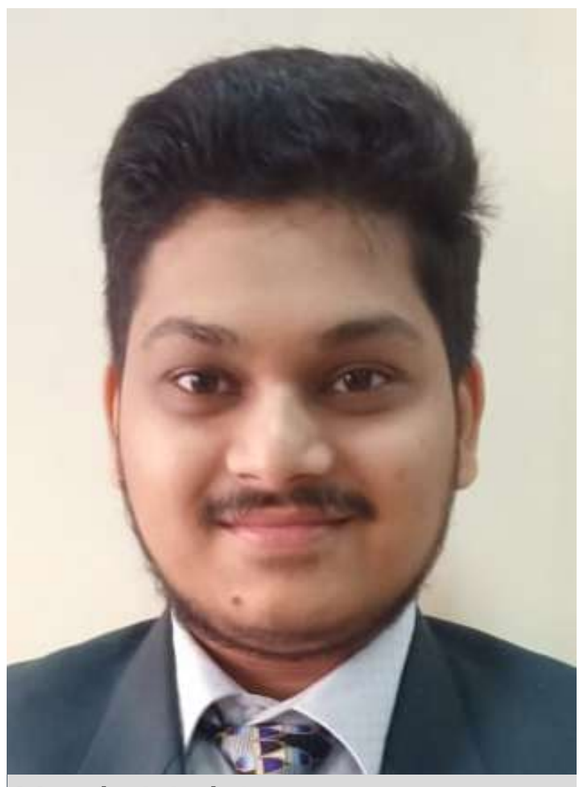
College festivals and sport days: D

• What is your valuable suggestion for the budding engineers?

Find your interest first and start working on that. Now a days everything is available online, just learn how and what to google: D

Tarang Marolikar
Editing Team

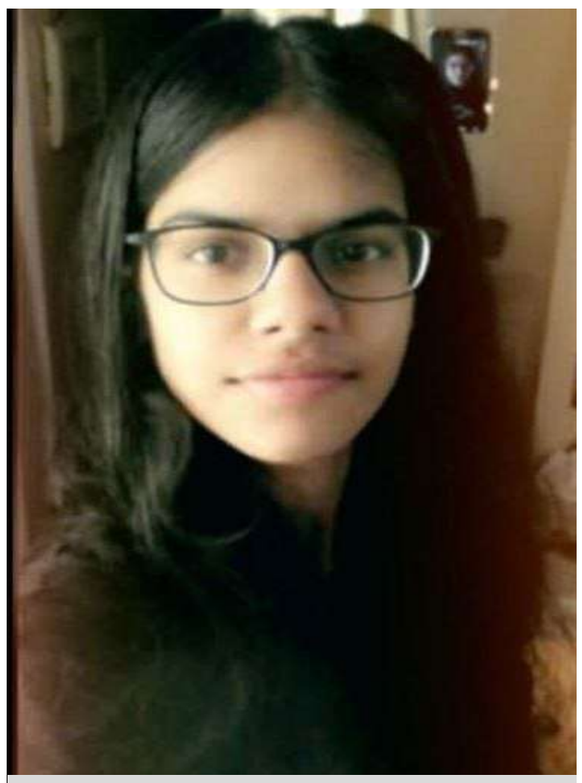
Students updating the ETA wall



Yash Mehta
Designing Team

Kushal Raut
Joint Secretory

Nihal Kumar
Secreatry



Prachi Purohit
ETA Wall Team

Shamini Iyer
Publicity Team

Omkar Chaudhari
Publicity Team

Students updating the ETA wall

Sneha Jaiswal
Designing Team

T
A
T
E
A
M

If you put a key under the mat for the cops, a burglar can find it, too. Criminals are using every technology tool at their disposal to hack into people's accounts. If they know there's a key hidden somewhere, they won't stop until they find it.

-Tim Cook