CAPTCHA
Digital Magazine
2023-24

DHEENUL ISLAM SABHA GIRLS HIGHER SECONDARY SCHOOL
KANNUR CITY -670003

What is Cybersecurity and Why It is Important?

Cybersecurity is the protection to defend internet-connected devices and services from malicious attacks by hackers, spammers, and cybercriminals. The practice is used by companies to protect against phishing schemes, ransomware attacks, identity theft, data breaches, and financial losses.

Look around today's world, and you'll see that daily life is more dependent on technology than ever before. The benefits of this trend range from near-instant access to information on the Internet to the modern conveniences provided by smart home automation technology and concepts like the Internet of Things.

With so much good coming from technology, it can be hard to believe that potential threats lurk behind every device and platform. Yet, despite society's rosy perception of modern advances, cyber security threats presented by modern tech are a real danger.

A steady rise in cybercrime highlights the flaws in devices and services we've come to depend on. This concern forces us to ask what cyber security is, why it's essential, and what to learn about it.

So, what is cyber security and how serious are cyber security threats these days? Read on and see.

What is Cyber Security?

Cyber security is a discipline that covers how to defend devices and services from electronic attacks by nefarious actors such as hackers, spammers, and cybercriminals. While some components of cyber security are designed to strike first, most of today's professionals focus more on determining the best way to defend all assets, from computers and smartphones to networks and databases, from attacks.

Cyber security has been used as a catch-all term in the media to describe the process of protection against every form of cybercrime, from identity theft to international digital weapons. These labels are valid, but they fail to capture the true nature of cyber security for those without a computer science degree or experience in the digital industry.

Cisco Systems, the tech conglomerate specializing in networking, the cloud, and security, defines cyber security as “…the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.”

Why is Cybersecurity Important?

In today's digital world, one cannot ignore cybersecurity. One single security breach can lead to exposing the personal information of millions of people. These breaches have a strong financial impact on the companies and also loss of the trust of customers. Hence, cyber security is very essential to protect businesses and individuals from spammers and cyber criminals.

The Scale of the Cyber Security Threat

According to Forbes, 2022 will present us with a pack of diverse and terrifying cyber security challenges, everything from supply chain disruption to increased smart device risks to a continued cyber security talent drought.

According to Cybercrime Magazine, cybercrime will cost the world $10.5 trillion annually by 2025! Furthermore, global cybercrime costs are predicted to rise by almost 15 percent yearly over the next four years.

Concepts such as the pandemic, cryptocurrency, and the rise in remote working are coming together to create a target-rich environment for criminals to take advantage of.

Types of information security threats

1. Insider threats

An insider threat occurs when individuals close to an organization who have authorized access to its network intentionally or unintentionally misuse that access to negatively affect the organization's critical data or systems.

Careless employees who don't comply with their organizations' business rules and policies cause insider threats. For example, they may inadvertently email customer data to external parties, click on phishing links in emails or share their login information with others. Contractors, business partners and third-party vendors are the source of other insider threats.

Some insiders intentionally bypass security measures out of convenience or ill-considered attempts to become more productive. Malicious insiders intentionally elude cybersecurity protocols to delete data, steal data to sell or exploit later, disrupt operations or otherwise harm the business.

2. Viruses and worms

Viruses and worms are malicious software programs (malware) aimed at destroying an organization's systems, data and network. A computer virus is a malicious code that replicates by copying itself to another program, system or host file. It remains dormant until someone knowingly or inadvertently activates it, spreading the infection without the knowledge or permission of a user or system administration.

A computer worm is a self-replicating program that doesn't have to copy itself to a host program or require human interaction to spread. Its main function is to infect other computers while remaining active on the infected system. Worms often spread using parts of an OS that are automatic and invisible to the user. Once a worm enters a system, it immediately starts replicating itself, infecting computers and networks that aren't adequately protected.

3. Botnets

A botnet is a collection of Internet-connected devices, including PCs, mobile devices, servers and IoT devices that are infected and remotely controlled by a common type of malware.

Typically, the botnet malware searches for vulnerable devices across the internet. The goal of the threat actor creating a botnet is to infect as many connected devices as possible, using the computing power and resources of those devices for automated tasks that generally remain hidden to the users of the devices.

The threat actors -- often cybercriminals -- that control these botnets use them to send email spam, engage in click fraud campaigns and generate malicious traffic for distributed denial-of-service attacks.

4. Drive-by download attacks

In a drive-by download attack, malicious code is downloaded from a website via a browser, application or integrated OS without a user's permission or knowledge. A user doesn't have to click on anything to activate the download. Just accessing or browsing a website can start a download.

Cybercriminals can use drive-by downloads to inject banking Trojans, steal and collect personal information as well as introduce exploit kits or other malware to endpoints.

5. Phishing attacks

Phishing attacks are a type of information security threat that employs social engineering to trick users into breaking normal security practices and giving up confidential information, including names, addresses, login credentials, Social Security numbers, credit card information and other financial information.

In most cases, hackers send out fake emails that look as if they're coming from legitimate sources, such as financial institutions, eBay, PayPal -- and even friends and colleagues.

In phishing attacks, hackers attempt to get users to take some recommended action, such as clicking on links in emails that take them to fraudulent websites that ask for personal information or install malware on their devices. Opening attachments in emails can also install malware on users' devices that are designed to harvest sensitive information, send out emails to their contacts or provide remote access to their devices.

6. Distributed denial-of-service attacks

In a distributed denial-of-service (DDoS) attack, multiple compromised machines attack a target, such as a server, website or other network resource, making the target totally inoperable. The flood

of connection requests, incoming messages or malformed packets forces the target system to slow down or to crash and shut down, denying service to legitimate users or systems.

7. Ransomware

In a ransomware attack, the victim's computer is locked, typically by encryption, which keeps the victim from using the device or data that's stored on it. To regain access to the device or data, the victim has to pay the hacker a ransom, typically in a virtual currency such as Bitcoin. Ransomware can be spread via malicious email attachments, infected software apps, infected external storage devices and compromised websites.attachments from unknown sources. Victims should do everything possible to avoid paying ransom.

Organizations should also couple a traditional firewall that blocks unauthorized access to computers or networks with a program that filters web content and focuses on sites that may introduce malware. In addition, limit the data a cybercriminal can access by segregating the network into distinct zones, each of which requires different credentials.

8. Exploit kits

An exploit kit is a programming tool that enables a person without any experience writing software code to create, customize and distribute malware. Exploit kits are known by a variety of names, including *infection kit*, *crimeware kit*, *DIY attack kit* and *malware toolkit*. Cybercriminals use these toolkits to attack system vulnerabilities to distribute malware or engage in other malicious activities, such as stealing corporate data, launching denial of service attacks or building botnets.

9. Malvertising

Malvertising is a technique cybercriminals use to inject malicious code into legitimate online advertising networks and web pages. This code typically redirects users to malicious websites or installs malware on their computers or mobile devices. Users' machines may get infected even if they don't click on anything to start the download.

Cybercriminals may use malvertising to deploy a variety of moneymaking malware, including cryptomining scripts, ransomware and banking Trojans.

Artificial Intelligence

What it is and why it matters

Artificial Intelligence History

The term artificial intelligence was coined in 1956, but AI has become more popular today thanks to increased data volumes, advanced algorithms, and improvements in computing power and storage.

Early AI research in the 1950s explored topics like problem solving and symbolic methods. In the 1960s, the US Department of Defence took interest in this type of work and began training computers to mimic basic human reasoning. For example, the Defence Advanced Research Projects Agency (DARPA) completed street mapping projects in the 1970s. And DARPA produced intelligent personal assistants in 2003, long before Siri, Alexa or Cortana were household names.

This early work paved the way for the automation and formal reasoning that we see in computers today, including decision support systems and smart search systems that can be designed to complement and augment human abilities.

While Hollywood movies and science fiction novels depict AI as human-like robots that take over the world, the current evolution of AI technologies isn't that scary – or quite that smart. Instead, AI has evolved to provide many specific benefits in every industry. Keep reading for modern examples of artificial intelligence in health care, retail and more.

Why is artificial intelligence important?

AI automates repetitive learning and discovery through data. Instead of automating manual tasks, AI performs frequent, high-volume, computerised tasks. And it does so reliably and without fatigue. Of course, humans are still essential to set up the system and ask the right questions.

AI adds intelligence to existing products. Many products you already use will be improved with AI capabilities, much like Siri was added as a feature to a new generation of Apple products. Automation, conversational platforms, bots and smart machines can be combined with large amounts of data to improve many technologies. Upgrades at home and in the workplace, range from security intelligence and smart cams to investment analysis.

AI adapts through progressive learning algorithms to let the data do the programming. AI finds structure and regularities in data so that algorithms can acquire skills. Just as an algorithm can teach itself to play chess, it can teach itself what product to recommend next online. And the models adapt when given new data.

AI analyses more and deeper data using neural networks that have many hidden layers. Building a fraud detection system with five hidden layers used to be impossible. All that has changed with incredible computer power and big data. You need lots of data to train deep learning models because they learn directly from the data.

AI achieves incredible accuracy through deep neural networks. For example, your interactions with Alexa and Google are all based on deep learning. And these products keep getting more accurate the more you use them. In the medical field, AI techniques from deep learning and object recognition can now be used to pinpoint cancer on medical images with improved accuracy.

AI gets the most out of data. When algorithms are self-learning, the data itself is an asset. The answers are in the data – you just have to apply AI to find them. Since the role of the data is now more important than ever, it can create a competitive advantage. If you have the best data in a competitive industry, even if everyone is applying similar techniques, the best data will win. But using that data to innovate responsibly requires trustworthy AI. And that means your AI systems should be ethical, equitable and sustainable.

AI has been an integral part of SAS software for years. Today we help customers in every industry capitalise on advancements in AI, and we'll continue embedding AI technologies like machine learning and deep learning in solutions across the SAS port.

Jim Goodnight CEO SAS

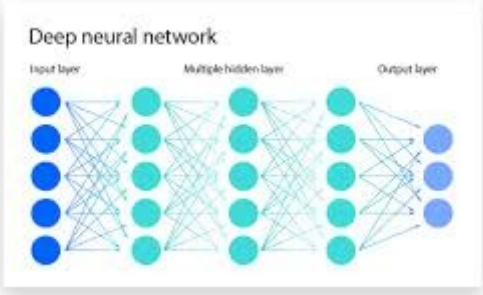
How Artificial Intelligence Works

AI works by combining large amounts of data with fast, iterative processing and intelligent algorithms, allowing the software to learn automatically from patterns or features in the data. AI is a broad field of study that includes many theories, methods, and technologies, as well as the following major subfields:

Machine Learning

Machine learning is a method of data analysis that automates analytical model building. It is a branch of artificial intelligence based on the idea that systems can learn from data, identify patterns and make decisions with minimal human intervention.

Neural Networks



Neural networks are computing systems with interconnected nodes that work much like neurons in the human brain. Using algorithms, they can recognise hidden patterns and correlations in raw data, cluster and classify it, and – over time – continuously learn and improve.

Deep Learning

Deep learning is a subset of machine learning that trains a computer to perform human-like tasks, such as speech recognition, image identification and prediction making. It improves the ability to classify, recognise, detect and describe using data. The current interest in deep learning is due, in part, to the buzz surrounding artificial intelligence (AI).

In summary, the goal of AI is to provide software that can reason on input and explain on output. AI will provide human-like interactions with software and offer decision support for specific tasks, but it’s not a replacement for humans – and won’t be anytime soon.

What is AI Security?

Artificial intelligence (AI) has revolutionized various industries, and cybersecurity is no exception. AI security solutions have emerged as powerful tools for identifying and mitigating potential threats in today's digital landscape. By leveraging machine learning algorithms and deep learning techniques, AI can analyze vast amounts of data, detect malicious behaviors, and provide organizations with enhanced protection against cyberattacks. In this article, we will explore the concept of AI security, its common applications, the benefits it offers, and key considerations when evaluating AI cybersecurity vendors.

understanding AI Security: Definition and Explanation

On a basic level, artificial intelligence (AI) security solutions are programmed to identify “safe” versus “malicious” behaviors by cross-comparing the behaviors of users across an environment to those in a similar environment. This process is often referred to as “unsupervised learning” where the system creates patterns without human supervision. For some AI platforms, like Vectra, “deep learning” is another key application for identifying malicious behaviors. Inspired by the biological structure and function of neurons in the brain, deep learning relies on large, interconnected networks of artificial neurons. These neurons are organized into layers, with individual neurons connected to one another by a set of weights that adapt in response to newly arriving inputs.

Sophisticated AI cybersecurity tools have the capability to compute and analyze large sets of data allowing them to develop activity patterns that indicate potential malicious behavior. In this sense, AI emulates the threat-detection aptitude of its human counterparts. In cybersecurity, AI can also be used for automation, triaging, aggregating alerts, sorting through alerts, automating responses, and more. AI is often used to augment the first level of analyst work.

Common Applications of AI in Cybersecurity

AI security solutions have a wide range of applications in the realm of cybersecurity. Here are some of the most common uses:

1. **Threat Detection and Prediction**: AI can analyze large datasets to identify activity patterns indicative of potential malicious behavior. By learning from previously detected behaviors, AI systems can autonomously predict and detect emerging threats.
2. **Behavior Contextualization and Conclusion**: AI can contextualize and draw conclusions from incomplete or new information, aiding in the identification and understanding of cybersecurity events.
3. **Remediation Strategy Development**: AI tools can suggest viable remediation strategies to mitigate threats or address security vulnerabilities based on their analysis of detected behaviors.
4. **Automation and Augmentation**: AI can automate various cybersecurity tasks, including alert aggregation, sorting, and response. It complements the work of human analysts, enabling them to focus on more complex challenges.

Benefits of Leveraging AI Technologies in Security

The adoption of AI cybersecurity solutions offers several advantages for organizations and their IT and security teams:

1. **Enhanced Data Processing**: AI's capabilities enable the processing of large volumes of data at high speed, providing organizations with comprehensive insights into potential threats.
2. **Augmentation for Resource-Constrained Teams**: AI fills the resource gap for smaller or less resourced cybersecurity teams by automating routine tasks and providing continuous protection.
3. **Consistent and Long-Term Protection**: AI systems provide consistent and continuous protection, reducing the risk of human error and offering long-term defense against evolving threats.

How CAPTCHAs work,What does CAPTCHA mean?

What is a CAPTCHA?

A CAPTCHA test is designed to determine if an online user is really a human and not a ot.b CAPTCHA is an acronym that stands for "Completely Automated Public Turing test to tell Computers and Humans Apart." Users often encounter CAPTCHA and reCAPTCHA tests on the Internet. Such tests are one way of managing bot activity, although the approach has its drawbacks.

Although CAPTCHAs are designed to block automated bots, CAPTCHAs are themselves automated. They're programmed to pop up in certain places on a website, and they automatically pass or fail users.

How does a CAPTCHA work?

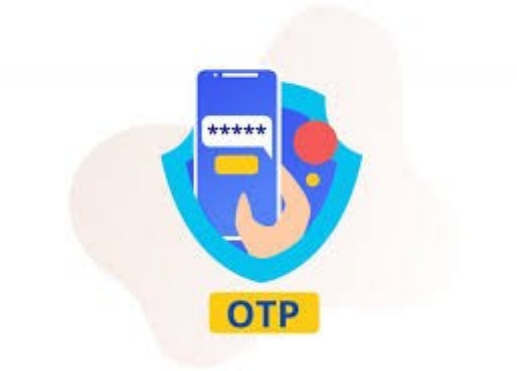
Classic CAPTCHAs, which are still in use on some web properties today, involve asking users to identify letters. The letters are distorted so that bots are not likely to be able to identify them. To pass the test, users have to interpret the distorted text, type the correct letters into a form field, and submit the form. If the letters don't match, users are prompted to try again. Such tests are common in login forms, account signup forms, online polls, and e-commerce checkout pages.

The idea is that a computer program such as a bot will be unable to interpret the distorted letters, while a human being, who is used to seeing and interpreting letters in all kinds of contexts – different fonts, different handwritings, etc. – will usually be able to identify them.

The best that many bots will be able to do is input some random letters, making it statistically unlikely that they will pass the test. Thus, bots fail the test and are blocked from interacting with the website or application, while humans are able to continue using it like normal.

Advanced bots are able to use machine learning to identify these distorted letters, so these kinds of CAPTCHA tests are being replaced with more complex tests. Google reCAPTCHA has developed a number of other tests to sort out human users from bots.

One Time Password (OTP, TOTP) : definition, examples



One-time password (OTP) systems provide a mechanism for logging on to a network or service using **a unique password that can only be used once**, as the name suggests.

Why is a one-time password safe?

The OTP feature prevents some forms of identity theft by making sure that a captured username/password pair cannot be used a second time.

Typically the user's login name stays the same, and the one-time password changes with each login.

One-time passwords (aka One-time passcodes) are a form of **strong authentication**, providing much better protection to eBanking, corporate networks, and other systems containing sensitive data.

OTP and TOTP vs static password

Although this authentication method is convenient, it is not secure because online identity theft – using phishing, keyboard logging, man-in-the-middle attacks, and other practices – is increasing worldwide.

Robust authentication systems address the limitations of static passwords by incorporating an additional security credential, such as a temporary one-time password (OTP), to protect network access and end-users' digital identities.

This feature adds extra protection and makes it more challenging to access unauthorized information, networks, or online accounts.

Time-based One-Time Password (TOTP) changes after a set period, such as 60 seconds.

The Role of OTP SMS in Banking Security

1. Protection Against Phishing Attacks

Phishing attacks have become increasingly common in the digital landscape. These attacks involve fraudsters tricking users into revealing their personal information or login credentials. OTP SMS plays a vital role in protecting against phishing attacks. By requiring users to enter the one-time password sent via SMS, banks can verify the authenticity of the user and prevent unauthorized access to their accounts.

2. Safeguarding Against SIM Swapping Attacks

SIM swapping attacks have emerged as a major threat to banking security. In these attacks, fraudsters manipulate telecommunication providers to issue replacement SIM cards for targeted users. By doing so, they gain access to the OTP SMS sent to the victim's mobile phone. Implementing OTP SMS in banking transactions helps protect against SIM swapping attacks, as the fraudsters would need physical access to the victim's phone to complete the transaction.

3. Mitigating Risks Associated with Android Platform Features

The Android platform, although widely used, poses certain risks when it comes to banking security. Malicious applications can exploit vulnerabilities in the platform, intercepting SMS messages and compromising user data. OTP SMS helps mitigate these risks by providing an additional layer of authentication that is independent of the device's operating system.

4. Addressing Insecure Telco Infrastructure

The infrastructure behind SMS communication is not entirely secure. SMS messages can travel through the cellular network unencrypted and may be stored in telco databases without encryption. OTP SMS can help address these vulnerabilities by ensuring that the passcode is sent securely to the user's mobile phone, minimizing the risk of interception or unauthorized access.

The Significance of OTP SMS in Banking

OTP SMS has become an integral part of the banking industry, serving as a crucial security measure for various types of transactions. Let's explore some scenarios where OTP SMS is mandatory:

Debit Card Transactions

When making online purchases using a debit card, customers are required to enter the OTP received via SMS API to complete the transaction. This ensures that only the authorized cardholder can initiate and authenticate the payment, minimizing the risk of fraudulent activities.

Credit Card Usage

Similar to debit cards, credit card transactions often involve the use of OTP SMS for added security. Banks send OTPs to their cardholders to verify and authorize transactions, protecting against unauthorized usage and potential fraud.

Internet Banking

Internet banking has revolutionized the way customers manage their finances, providing convenience and flexibility. However, it also introduces potential security risks. OTP SMS serves as a safeguard by implementing two-factor authentication, where customers must enter the OTP received via SMS in addition to their login credentials. This ensures that only authorized individuals can access and perform transactions on their accounts.

Advantages and Limitations of OTP SMS

While OTP SMS has gained widespread acceptance and usage, it is essential to consider its advantages and limitations in the context of security and user experience.

Advantages of OTP SMS

- **Wide Accessibility:** OTP SMS is accessible to all users with a mobile phone, regardless of their device or internet connectivity. This makes it an inclusive security measure that can reach a broad user base.
- **No Additional App Required:** Unlike other authentication methods that require users to download specific apps, OTP SMS leverages the inherent messaging capabilities of mobile phones, eliminating the need for additional installations.
- **Real-time Authentication:** The instant delivery of OTP SMS ensures that users receive the authentication code promptly, enabling seamless and timely transaction verifications.

Limitations of OTP SMS

- **Vulnerability to Phishing Attacks:** OTP SMS can be susceptible to phishing attacks, where fraudsters attempt to deceive users into revealing their OTP codes through fraudulent websites or social engineering tactics. Users must exercise caution and ensure they only enter OTP codes on trusted platforms.
- **Dependency on Telecommunication Services:** Banks rely on telecommunication services to deliver OTP SMS to their customers. However, the dependency on third-party providers introduces potential vulnerabilities, such as SIM swapping attacks and interception of SMS messages.
- **Inconvenience and User Experience:** Users may find the process of manually entering OTP codes for each transaction time-consuming and inconvenient, especially when completing multiple transactions in quick succession. Additionally, factors such as network issues or delays in SMS delivery can impact the user experience.
  One should always adhere to the guidelines for OTP SMS fraud prevention.

സൈബർ ലോകം...എന്തൊക്കെയാണ് സുരക്ഷാ മാർഗ്ഗങ്ങൾ?

“ഡിജിറ്റൽ ഇന്ത്യ” “കേരളം – നൂറു ശതമാനം ഡിജിറ്റൽ സാക്ഷരത സംസ്ഥാനം” എന്നീ മുദ്രാവാക്യങ്ങൾ ഭാരതത്തിന്റെ രണ്ടു ദശാബ്ദം നീണ്ട ഇൻഫർമേഷൻ ടെക്നോളജിയിലെ സ്ഥിരതയാർന്ന കുതിപ്പിന്റെയും,അതിന്റെ മികവാർന്ന ടെക്നോളജിസ്റ്റുകളുടെ നിരന്തര പരിശ്രമത്തിന്റെയും,ഭരണകർത്താക്കളുടെ ദീർഘവീക്ഷണത്തിന്റെയുംപരിണിതഫലമായിട്ടുണ്ടായിട്ടുള്ളതാണ്.

എന്നാൽ എല്ലാവിധത്തിലുള്ള ഡിജിറ്റൽ വികസനത്തിന്റെയും,ഗ്രാമങ്ങളെയും, സർക്കാർ സംവിധാനങ്ങളെയും, പൌരന്മാരുടെ വ്യക്തിഗതവിവരങ്ങളും, സാമ്പത്തിക ഇടപാടുകളും “ഓൺലൈൻ” ആക്കുമ്പോൾ,വിവരസുരക്ഷയുടെയും, സൈബർ സുരക്ഷയുടെയും കാര്യത്തിലുള്ള സമഗ്രമായ ഒരു സമീപനം നമുക്ക് അത്യാവശ്യമാണ്. ഇനിയുള്ള ദിനങ്ങൾ,രാജ്യങ്ങൾ തമ്മിലുള്ള യുദ്ധങ്ങൾ പോലും, കരയും, കടലും, ആകാശവുംകടന്നു, സൈബർ ലോകത്തിലായിരിക്കും എന്നതിനെ കുറിച്ച് മനസ്സിലാക്കി,സർക്കാരുകൾ മുൻകൂട്ടി പ്രവർത്തിക്കാനുള്ള നടപടികൾ സ്വീകരിക്കണം എന്നാണ് ഈ രംഗത്ത് ഒരു പാട് കാലത്തെ അനുഭവജ്ഞാനം ഉള്ള വിദഗ്ധർ അഭിപ്രായപെടുന്നത്. ഇന്ന് നടക്കുന്ന “ഫയർ ഫയിറ്റിഗ്” (Fire Fighting) സുരക്ഷാ പ്രശ്നങ്ങൾ നടന്ന ശേഷമുള്ള ചില നടപടിക്രമങ്ങൾ മാത്രമാണ്.സൈബർ ആക്രമണങ്ങളും, വിവരചോരണങ്ങളും, രാജ്യത്തിന്റെയും സംസ്ഥാനങ്ങളുടെയും, ജനങ്ങളുടെയും ജീവനും സ്വത്തിനും വരെ ഭീഷണിയായി മാറിക്കൊണ്ടിരിക്കുന്ന കാര്യം, ഇത് എത്രമാത്രംസൂക്ഷ്മതയോടു കൂടി കൈകാര്യം ചെയ്യണം എന്നത് ഒന്ന് കൂടി നമ്മളെ ഓർമ്മിപ്പിക്കുന്നു.

സൈബർ സുരക്ഷ പ്രശ്നങ്ങൾ പല തലത്തിലും തരത്തിലും കാണപ്പെടുന്നുണ്ടെങ്കിലും, അതിനെ അതിജീവിക്കൽ, നമ്മൾ എത്രമാത്രം വിപുലമായ രീതിയിൽ സുരക്ഷ നടപടികൾ ചെയ്തിട്ടുണ്ട് എന്നതിനെ ആശ്രയിച്ചിരിക്കും...

ഇനി ഒരു പക്ഷെ എല്ലാ സുരക്ഷ ക്രമീകരണങ്ങളും ചെയ്തിട്ടുണ്ടെങ്കിലും അതിനെയും തകർത്ത് നാശം വിതക്കാൻ മാത്രം ശക്തമായ ആക്രമണങ്ങൾ നടത്താനും തയ്യാറുള്ള കറുത്ത ശക്തികൾ (Dark forces) വിഹരിച്ചു നടക്കുന്ന സ്ഥലമാണ് സൈബർ ലോകം.

സ്ഥാപനങ്ങളും വ്യക്തികളും രാഷ്ട്രങ്ങളും സൈബർക്രിമിനലുകളുടെ പലവിധ താൽപ്പര്യങ്ങളുടെയും ആക്രമണങ്ങളുടെയും ഇരകളായി കൊണ്ടിരിക്കുന്ന ഈ കാലഘട്ടത്തിൽ, കേരളം പോലെ സാങ്കേതിക അതിൻറെ സമഗ്രത ഉറപ്പു വരുത്തും. അതിനു മാത്രമേ സുദീർഘവും സുശക്തവുമായ സുരക്ഷ ഉറപ്പു വരുത്താൻ പറ്റും എന്നുള്ളതാണ് വസ്തുത.

വിവര സുരക്ഷയുടെ പ്രാധാന്യം ഇന്നും വേണ്ട വിധത്തിൽ മനസ്സിലാക്കിയിട്ടുണ്ടോ ലോകമാകയുള്ള പൊതു സമൂഹവും,സ്ഥാപനങ്ങളും, സർക്കാരുകളും എന്നത് ഒരു ചിന്തനീയമായ കാര്യം.സാമ്പത്തിക സ്ഥാപനങ്ങളും മറ്റും ഒരു പരിധി വരെ സുരക്ഷക്രമീകരണങ്ങൾ ഉറപ്പാക്കുന്നതിൽ ജാഗ്രത പുലർത്തുന്നുണ്ട്. വിദ്യയുടെ ഉപയോഗം ജീവിതത്തിൻറെ എല്ലാ മേഖലയിലും പ്രതിഫലിച്ച ഒരു സമൂഹത്തിൽ അതിന്റെ പ്രത്യാഘാതങ്ങൾ വളരെ വലുതാണ്..

പക്ഷെ വളരെ ശ്രദ്ധേയവും ഭീതിജനകവുമായ കാര്യം, ഇനിയും നമ്മൾ ഇത്തരത്തിലുള്ള ആക്രമണങ്ങളെ അതിൻറെ ശരിയായ ഗൌരവത്തിൽ ഉൾക്കൊണ്ടു കൊണ്ട് നേരിടാനുള്ള യാതൊരു വിധത്തിലുള്ള പ്രായോഗികവും ഫലപ്രദവുമായ തയ്യാറെടുപ്പുകളോ സുരക്ഷക്രമീകരണങ്ങളോ നടത്തിയിട്ടില്ല എന്നതാണ്.

ഏറ്റവും അവബോധം ഉള്ള വ്യക്തികളെയും സ്ഥാപനങ്ങളെയും പോലും കെണിയിൽ പെടുത്തുന്ന തരത്തിലുള്ള “സ്കാമുകളും”, ചതികളിൽ വീഴാതെ രക്ഷപെട്ടു നടക്കുന്നവരെ പോലും വീഴ്ത്തുന്ന “സ്പാമുകളും”,സുരക്ഷ ക്രമീകരണങ്ങൾ പലതും ചെയ്ത കമ്പ്യൂട്ടർകളെ പോലും തകർക്കുന്ന “വേമുകളും (worm)” അതിവേഗത്തിൽ വ്യാപിച്ചു കൊണ്ടിരിക്കുന്ന സാഹചര്യമാണ് ഇന്ന് സൈബർ ലോകത്തുള്ളത്.കമ്പ്യൂട്ടർ സുരക്ഷാ ഭീഷണികൾ പുറത്തു നിന്നും ഉള്ള പോലെ തന്നെ പലപ്പോഴും അകത്തു നിന്നും പ്രതീക്ഷിക്കാവുന്ന തരത്തിലാണ് സ്ഥാപനങ്ങളും സർക്കാരുകളും പ്രതിരോധം തീർക്കേണ്ടതായിട്ടുള്ളത്.

സുരക്ഷക്ക് ഭീഷണിയാകുന്ന കാര്യത്തിൽ ദൌർബല്യങ്ങൾക്ക് എന്നും പ്രധാന പങ്കുണ്ട് എന്നുള്ളത് ഒരു വസ്തുതയാണ്. അത് വ്യക്തികളുടെയും, സർക്കാർസ്ഥാപനങ്ങളുടെയും സർക്കാരിതര സ്ഥാപനങ്ങളുടെയും സുരക്ഷയാണെങ്കിലും വ്യത്യസ്തമല്ല.യഥാർത്ഥത്തിൽ സുരക്ഷയുടെ കാതൽ എന്ന് പറയുന്നത്, ഓരോസ്ഥാപനങ്ങളിലെയും, അതുമായി ബന്ധപെട്ട വ്യക്തികളുടെയും അതിന്റെപ്രവർത്തനങ്ങളിലെയും ദൌർബല്യങ്ങൾ യഥാവിധം മനസ്സിലാക്കി അനുയോജ്യമായ മുൻകരുതലുകൾ എടുക്കുക എന്നതാണ്. സ്വകാര്യതകളിലും അല്ലാത്ത കാര്യങ്ങളിലും അത് എത്ര മാത്രം അടച്ചുറപ്പോടെ ചെയ്യുന്നു എന്നത് സൈബർ സുരക്ഷയിലും വിവര സുരക്ഷയിലും വളരെ അധികം ഗൌരവത്തോടെ കാണേണ്ട ഒരു വിഷയമാണ്.നിലവിലുള്ള സുരക്ഷാ നടപടികൾ എത്രമാത്രം ഫലപ്രദം എന്നത് വളരെ പ്രായോഗികമായി

വിലയിരുത്തി കൂടുതൽ ശക്തവും ഫലപ്രദവും ആയ രീതിയിൽ നടപ്പിൽ വരുത്തേണ്ടതുണ്ട്. സർക്കാരിന്റെ വ്യക്തവും കണിശവുമായ ഇടപെടൽ ഇതിൽ വളരെ പ്രാധാന്യം അർഹിക്കുന്ന കാര്യമാണ്.

പലപ്പോഴും സ്ഥാപനങ്ങളും സർക്കാരുകളും ജാഗ്രതകരാകുന്നത് ഒരു സൈബർ ആക്രമണമോ, നഴഞ്ഞു കയറ്റമോ, വിവരചോരണമോ (Information Leakage) സംഭവിക്കുമ്പോൾ മാത്രമാണ്. സുരക്ഷയുടെ അതീവപ്രാധാന്യം മനസ്സിലാക്കാതിരിക്കുകയും, മറ്റു പല തിരക്കുകളും കൊണ്ട് അതിനെ അവഗണിക്കുകയും ആണ് പൊതുവിൽ കാണുന്ന ഒരു സമീപനം.

മറ്റൊരു പ്രധാനപെട്ട വിഷയം, വിവര സുരക്ഷയും സൈബർ സുരക്ഷയും വെറും സാങ്കേതികതയുടെയും ഉപരിപ്ലവവും നാമമാത്രമായ ചില നിയന്ത്ര മാത്രമായി അവശേഷിക്കാതിരിക്കാൻ ശ്രദ്ധിക്കുക എന്നതാണ്..സാങ്കേതിക വിദ്യ, സുരക്ഷയിലെ ഒരു നെടുംതൂൺ ആണെങ്കിലും, ഭദ്രവും എല്ലാ തലങ്ങളിലും സ്പർശിക്കുന്നതുമായ സുരക്ഷാക്രമീകരണങ്ങൾ സൈബർ സുരക്ഷയിലും വിവരസുരക്ഷയിലും ന്ന എന്നുള്ളത് ശ്ലാഘനീയമാണ്.

വിവരസുരക്ഷയുടെ കാതലായ കാര്യം നേരത്തെ പറഞ്ഞ പോലെ അതിന്റെ സമഗ്രതയിലാണ്. അതിലേക്കായി ചില നിർദ്ദേശങ്ങൾ താഴെ സ്ഥാപനങ്ങളും സർക്കാരുകളും വിവരസുരക്ഷയ്ക്കായ് വളരെ വിപുലമായ പഠനങ്ങൾ നടത്തിയ ശേഷം കൃത്യമായ ലക്ഷ്യവും മാർഗ്ഗവും അതിന വേണ്ടിയുള്ള നയങ്ങളും രൂപികരിക്കേണ്ടതുണ്ട്. വിവരസുരക്ഷാസ്ട്രെജി (Strategy) രൂപീകരണം എത്ര മാത്രം ഗഹനമായും ദീർഘവീക്ഷണത്തോട് കൂടിയും നടത്തുന്ന എന്നത് അതിൻറെ വിജയ നിദാനം തന്നെ ആണ്.

വിവരസുരക്ഷയുടെ എല്ലാ തലങ്ങളിലും വിപുലവും അഗധവുമായ അനുഭവപരിചയമുള്ള വിദഗ്ദരുടെ നേതൃത്വവും, സർക്കാരിന്റെയോസ്ഥാപനങ്ങളുടെയോ ഉന്നതരുടെ വിട്ടുവീഴ്ചയില്ലാത്ത പിന്തുണയും വിജയകരമായ ദൗത്യത്തിന് വളരെ പ്രധാനമാണ്.

വിദഗ്ധരുടെ സഹായത്തോടെ സ്ട്രാറ്റെജിയും (strategy), അതിനനുസൃതമായി;സർക്കാർ തലത്തിലോ സ്ഥാപന തലത്തിലോ ഉള്ള നയരൂപികരണവും നടപടികളും ക്രമപെടുത്തുകയാണ് അടുത്തതായി ചെയ്യേണ്ടത്. ആഗോളതലത്തിൽ തന്നെ വളരെ പ്രബലവും സ്വീകാര്യതയും ഉള്ള മാനദണ്ഡങ്ങൾ(standards) ഇതിനു വേണ്ടി സ്വീകരിക്കാവുന്നതുമാണ്. ISO 27001, NIST, PCI-DSS തുടങ്ങിയവ ഇതിലെ പ്രധാനപെട്ടവയാണ്. രൂപികരിക്കുന്ന നയങ്ങൾക്കും എടുക്കുന്ന നടപടികൾക്കും ഏകീകൃത സ്വഭാവവും സ്ഥിരതയും ദീർഘകാല നിലനിൽപ്പും ഉറപ്പു വരുത്താൻ ഇത് സഹായകമാകും.

അതിൽ നിന്നുള്ള നഷ്ടം (സാമ്പത്തികമോ, അല്ലാതെയോ ഉള്ള) എങ്ങനെ കുറയ്ക്കാം എന്നുള്ളതും സുസേവനങ്ങളുടെയും, വിവരവും,വിവരസാങ്കേതിക വിദ്യയുമായും ബന്ധപെട്ടു കിടക്കുന്ന എല്ലാവസ്തുക്കൾക്കുമുള്ള മൂല്യനിർണയവും, അവയ്ക്കുള്ള ദൌർബല്യങ്ങളും,ഭീഷണികളും, അപകടസാദ്ധ്യതകളും വളരെ വിശദമായും ഗഹനവുമായുംമനസ്സിലാക്കി നിയന്ത്രണങ്ങൾ കണ്ടെത്തി സ്ഥാപിക്കാൻ ഉള്ള ശ്രമങ്ങൾ വേണം.

സർക്കാർ തലത്തിൽ വളരെ വിപുലമായി മുകളിൽ പറഞ്ഞ ഒരു ചട്ടക്കൂടും മാർഗ്ഗനിർദേശങ്ങളും എല്ലാ സ്ഥാപനങ്ങളിലും, എല്ലാ പദ്ധതികളിലും നിർബന്ധമായും ഉറപ്പു വരുത്തണം. എല്ലാ വിവരകൈമാറ്റങ്ങളും,പുറംലോകത്തേക്ക് പോകുന്ന വിവരങ്ങളും വളരെ ശ്രദ്ധയോടും,സൂക്ഷ്മതയോടും കൈകാര്യം ചെയ്യേണ്ടതും. എന്തൊക്കെ വിവരങ്ങൾ ഏതൊക്കെ തരത്തിൽ രാജ്യത്തിനും സർക്കാരുകൾക്കും ജനങ്ങൾക്കും പ്രാധാന്യം അർഹിക്കുന്നു എന്ന് നോക്കി തരം തിരിക്കുകയുംഅതിനനുസരിച്ച് സുരക്ഷാ കവചങ്ങൾ ഉറപ്പിക്കുകയും വേണം.വിവരസുരക്ഷയും സൈബർ സുരക്ഷയും പഠിപ്പിക്കുന്ന ചില ബാലപാഠങ്ങളുണ്ട്, ചില നിയന്ത്രണങ്ങൾ, പല തലത്തിലുള്ള സാങ്കേതിക മാർഗങ്ങൾ സുരക്ഷാ വിദഗ്ധരുടെ സഹായത്തോടു കൂടി സ്ഥാപിക്കുക.അവ എല്ലാ വിധത്തിലും പൂർണമായ തോതിൽ പ്രവർത്തിക്കുന്നുണ്ടെന്നും,അവയിൽ നിന്ന് കിട്ടുന്ന അടയാളങ്ങൾ, മുന്നറിയിപ്പുകൾ സ്ഥിരമായി വീക്ഷിക്കുകയും, സംശയാസ്പദമായ സാഹചര്യങ്ങളിൽ ഉടൻ പ്രതിരോധപ്രവർത്തനങ്ങൾ ഊട്ടി ഉറപ്പിക്കാനുള്ള നടപടികൾ തുടങ്ങണം.

സൈബർ സുരക്ഷയോ, വിവര സുരക്ഷയോ ഒരിക്കലും സാങ്കേതിക നിയന്ത്രങ്ങൾ കൊണ്ട് മാത്രം നേടാൻ സാധിക്കില്ല എന്ന കാര്യം വളരെ വ്യക്തമാണ്. സ്ഥാപനങ്ങളുടെയും, അവിടെ പ്രവർത്തിക്കുന്നവരുടെയും നടപടിക്രമങ്ങളും, ഉദ്യോഗസ്ഥരുടെയും ജനപ്രധിനിധികളുടെയും,ജനങ്ങളുടെയും സുരക്ഷാ അവബോധവും വളരെ പ്രധാനപെട്ട ഒരു ഘടകമാണ്. എന്തൊക്കെ സാമ്പത്തികവും സാങ്കേതികവുമായസംവിധാനങ്ങൾ ഉണ്ടെങ്കിലും, അവബോധത്തോടും ഉത്തരവാദിത്തത്തോടും കൂടിയും അവ ഉപയോഗിച്ചില്ലെങ്കിൽ, അവയൊക്കെ വെറും നോക്കുകുത്തികൾ ആയി മാറാൻ യാതൊരു തടസ്സവുമുണ്ടാകില്ല.

സമഗ്രവും, പഴുതുകളില്ലാത്തതുമായ പ്രതിരോധ സംവിധാനങ്ങൾ,അപായസാധ്യതകൾക്ക് അനുസൃതമായി ഉറപ്പു വരുത്തുകയും, അവ സ്ഥിരമായി പരിപാലിക്കുകയും, എല്ലാ കോണിൽകൂടിയുമുള്ള നിരീക്ഷണസംവിധാനം കുറ്റമറ്റതാക്കുകയും ചെയ്താൽ ഒരു പരിധി വരെ സുരക്ഷാപ്രശ്നങ്ങളിൽ നിന്ന് നമുക്ക് രക്ഷ നേടുകയും, സുരക്ഷാവിടവുകൾ നേരത്തെ മനസ്സിലാക്കി അതിനെ അടക്കാനുള്ള മറ്റു നിയന്ത്രണ മാർഗങ്ങൾ ഉറപ്പു വരുത്തുകയും ചെയ്യാം. ഇനി സുരക്ഷാ ആക്രമണങ്ങൾ എല്ലാനിയന്ത്രണങ്ങളും തകർത്തുവന്നാൽ അതിനെ എങ്ങിനെ നേരിടാം എന്നതുംരക്ഷാനയങ്ങളിലും നടപടികളിലും വ്യക്തമായി അടയാളപെടുത്തേണ്ടതാണ്.

അതിൽ ചിലപ്പോൾ, മറ്റൊരു സ്ഥലത്ത് മറ്റൊരു സർവർകളിൽ വെബ് സൈറ്റ് സ്ഥാപിക്കുന്നതുല്പ്പടെയുള്ള കാര്യങ്ങൾ ഉള്പെടാം

വ്യക്തികളുടെ സൈബർ സുരക്ഷക്ക് താഴെ പറയുന്ന കാര്യങ്ങളിൽ ശ്രദ്ധിക്കുക പ്രത്യേകിച്ചും, സാമൂഹ്യമാധ്യമങ്ങൾ ഉപയോഗിക്കുമ്പോൾ ഇതിലെ പല കാര്യങ്ങളിലും കൂടുതൽ സൂക്ഷ്മത പുലർത്തണം.

വ്യക്തിഗതമായ വിവരങ്ങൾ വളരെ ശ്രദ്ധയോട് കൂടി മാത്രം പൊതു മണ്ഡലത്തിൽ പങ്കു വെക്കുക.
സൈബർ ലോകം സ്വകാര്യതയിൽ കടന്നു കയറാനുള്ള അവസരംഉണ്ടാക്കനിട വരുത്താതെ നോക്കണം

യാതൊരു പരിചയവുമില്ലാത്ത ആൾക്കാരുമായി ഇടപഴകുമ്പോൾ വളരെയധികം മുൻകരുതലുകൾ എടുക്കുക. അങ്ങേ ഭാഗത്തുള്ളത് യഥാർത്ഥ വ്യക്തി തന്നെയാണോ എന്നത് എല്ലാ മാർഗങ്ങളുംഉപയോഗിച്ച് ഉറപ്പു വരുത്തണം. സാമൂഹ്യ മാധ്യമങ്ങൾ (ഫെയ്സ്ബൂക്, ട്വിറ്റെർ, യൂടുബ്....എന്നിങ്ങനെ) ഉപയോക്തൾക്ക് അവയുടെ ഉപയോഗം ഏറ്റവും എളുപ്പമാക്കാൻ, പല സുരക്ഷാമാനധണ്ടങ്ങളും കാറ്റിൽ പറത്തുകയാണ് പതിവ്. ആർക്കും, ഏതു പേരിലും, ഏതു കള്ള വ്യക്തിത്വത്തിലും കറങ്ങി നടക്കാൻ വളരെ എളുപ്പമാണ് ഇവിടെങ്ങളിൽ.

സത്യമാണെന്ന് ഉറപ്പുവരുത്തുന്നത് വരെ നിങ്ങൾ ഇന്റർനെറ്റ്-ൽ വായിക്കുന്നതും കേൾക്കുന്നതും, കാണുന്നതും വിശ്വസിക്കാ തിരിക്കുക. തെറ്റായ വിവരങ്ങളും, ചതിയിൽ പെടുത്താനുള്ള കെണികളും, തമാശകളും പറന്നു നടക്കുന്ന വിശാലമായ ഒരു ലോകമാണ് സൈബർ. 200 ശതമാനവും ആധികാരിതയും വ്യക്തിവിവരങ്ങളുടെ സത്യാവസ്ഥയും മനസ്സിലാക്കിയ ശേഷം മാത്രം കൂടുതൽ ഇടപെടലുകളും വിവരകൈമാറ്റവും നടത്താൻ വളരെ ബോധപൂർവ്വമായ ശ്രമം ഏതു സാഹചര്യത്തിലും ഉറപ്പുവരുത്തണം.

ഉപയോഗിക്കുന്ന സാമൂഹ്യമാധ്യമങ്ങളുടെ സുരക്ഷാക്രമീകരണങ്ങൾ മനസ്സിലാക്കുകയും അത് ഏറ്റവും സുരക്ഷിതമായ രീതിയിൽ ക്രമപെടുത്തി വെക്കുകയും ചെയ്യുക. സാധാരണഗതിയിൽ ഏറ്റവും സുരക്ഷ കുറഞ്ഞ രീതിയിലും മറ്റുള്ളവർക്ക് എളുപ്പത്തിൽ കിട്ടാവുന്ന രീതിയിലും ആയിരിക്കും ഇങ്ങനെയുള്ള വെബ് സൈറ്റ്കളും സോഫ്റ്റ്വെയർകളും തയ്യാറാക്കിയിരിക്കുക. ഉദാഹരണമായി ഫേസ്ബുക്ക് – നമ്മൾ മാറ്റുന്നത് വരെ ഏറ്റവും അയവുള്ളതും ശിഥിലവുമായ രീതിയിലായിരിക്കും സുരക്ഷാസ്ഥിതി. നമ്മൾ സുഹൃത്തുക്കൾക്ക് മാത്രം കാണാൻ പറ്റും എന്ന് കരുതുന്ന വിവരങ്ങളും ചിത്രങ്ങളും ലോകത്തിലെ ആർക്കു വേണമെങ്കിലുംകാണാനും എടുക്കാനും പറ്റുന്ന രീതിയിൽ!

ആയിരക്കണക്കിനുള്ള പുതിയതും പഴയതുമായ പ്രോഗ്രാമുകൾ നമ്മുടെ സ്വര്യജീവിതത്തിൽ സാമൂഹ്യമാധ്യമത്തിലൂടെയും അല്ലാതെയും കടന്നുവരും. ചിലത് ഉപകാരപ്രധമെങ്കിൽ മറ്റ് ചിലവ ഉപദ്രവകാരികളും ആണ്. ചിലവയുടെ പ്രവർത്തനങ്ങൾ നമ്മൾ അറിയാതെ നമ്മുടെ വിവരങ്ങളും ചെയ്യുന്ന കാര്യങ്ങളും അടക്കം ചോർത്തുന്ന തരത്തിലുമായിരിക്കാം. സൌജന്യമായി എന്ത് തരാം എന്ന് പറഞ്ഞാലും, ഏതു സോഫ്റ്റ്വയർ തരാം എന്ന് പറഞ്ഞാലും സംശയിക്കുക. ഏതെങ്കിലും തരത്തിൽ സാമ്പത്തിക ലാഭം ഇല്ലാതെ ആരും ഒന്നും സൌജന്യമായിതരില്ല എന്ന കാര്യം മനസ്സിൽ നൂറുശതമാനവും ഊട്ടി ഉറപ്പിക്കുക. ഒരിക്കൽ നമ്മൾ ശരി എന്ന് പറഞ്ഞ് സോഫ്റ്റ്വെയർ ഇൻസ്റ്റാൾ ചെയ്ത് കഴിഞ്ഞാൽ, പിന്നീട് നമ്മൾ അറിയാതെ തന്നെ നമ്മുടെ കമ്പ്യൂട്ടറിലെ വിവരങ്ങളും ഫയലുകളും പലയിടത്തും എത്തിയേക്കാം.. നമ്മുടെ കമ്പ്യൂട്ടറിലെ ക്യാമറയുടെ നിയന്ത്രണം പോലും ഏറ്റെടുത്ത് സ്വകാര്യതയുടെ എല്ലാ സീമകളും കടന്നേക്കാം. സൂക്ഷിച്ചാൽ ദുഖിക്കേണ്ട!

ഉപയോഗിക്കുന്ന പാസ്സ്വേർഡ്കളും മറ്റും ഏറ്റവും സങ്കീർണമായതു തന്നെ ആക്കാൻ ശ്രദ്ധിക്കണം. മാസത്തിൽ ഒരിക്കലെങ്കിലും പാസ്സ്വേർഡ് മാറ്റാൻ ശ്രമിക്കണം. ഇഷ്ടപെട്ട,ഓർമ്മയിൽ നിൽക്കുന്ന ഏതേലും ഗാനത്തിന്റെയൊ മറ്റേതെങ്കിലും വാചകങ്ങളുടെയൊ ആദ്യവരികളിലെ വാക്കുകളിലെ ആദ്യാക്ഷരങ്ങൾ ചേർത്ത് പാസ്സ്വേർഡ് ഉണ്ടാക്കിയാൽ സങ്കീർണതയും ഓർമിക്കാനുള്ള അനായാസതയും

ഒരുമിച്ച് കിട്ടും. അതെ പോലെ ഒരേ പാസ്സ്‌വേർഡ് എല്ലാ വിധ ആവശ്യങ്ങൾക്കും ഉപയോഗിക്കുന്നതിനു പകരം ചില തരംതിരിവ് നടത്തിയാൽ നല്ലതാണ്. സാമ്പത്തിക ഇടപാടുകൾക്ക് ഉപയോഗിക്കുന്ന പാസ്സ്‌വേർഡ്കൾ, സാമൂഹ്യ മാധ്യമങ്ങളുടെയൊ,ഇമെയില്കളുടെയോ ലോഗിൻ -ന വേണ്ടി ഉപയോഗിക്കതെയിരിക്കുന്നതാണ് നല്ലത്. അതേപോലെ ഓഫീസ് സംബന്ധമായി ഉപയോഗിക്കുന്നവ സ്വകാര്യവശ്യങ്ങളുമായി ബന്ധപെട്ട ഉപയോഗിക്കുന്നത് ഒഴിവാക്കിയാൽ പല സുരക്ഷാവീഴ്ച്ചകളിലും ആഘാതം കുറക്കാൻ സഹായകമാകും.

നിങ്ങൾ ഉപയോഗിക്കുന്ന കമ്പ്യൂട്ടർ ആകട്ടെ സ്മാർട്ട് ഫോൺ ആകട്ടെ, ഏറ്റവും പുതിയ സോഫ്റ്റ്‌വെയർഉം, ഏറ്റവും നല്ലസെക്യൂരിറ്റി സോഫ്റ്റ്‌വെയർ ഉം ഇൻസ്റ്റോൾ ചെയ്ത്, വളരെ ഫലപ്രദമായി ക്രമീകരിച്ചു ഉപയോഗിക്കാൻ ശ്രദ്ധിക്കുക.സൗജന്യമായതും പണം കൊടുത്തു വാങ്ങിക്കുന്നതുമായ നിരവധി നല്ലസോഫ്റ്റ്‌വെയർകൾ, ഇപ്പോൾ കിട്ടാനുണ്ട്. പക്ഷെ അതിലും കള്ളനാണയങ്ങൾ ഉണ്ട്. സോഫ്റ്റ്‌വയർ എടുക്കുന്നത് യഥാർത്ഥ വെബ്സൈറ്റ് ആണെന്നും, വിശ്വസനീയമായാതാണെന്നും ഉറപ്പു വരുത്തൽ വളരെ പ്രധാനമാണ്. വെറും ആന്റി വൈറസ് സോഫ്റ്റ്‌വെയർ മാത്രമല്ലാതെ, കളവ് പോകുന്നതിൽ നിന്നും, സ്വകാര്യത തകർക്കുന്നകാര്യങ്ങളിൽ നിന്നുമുള്ള രക്ഷക്കും സഹായകമായ വളരെ ഫലപ്രദമായ ചില സോഫ്റ്റ്‌വെയർകൾ ഇപ്പോൾ വളരെ അധികം ശ്രദ്ധേയമായി വരുന്നുണ്ട്.