Computer end user security (CEUSA)

I. Intro to Cyber Security

(.)

Cyber Security is a process that's designed to protect networks and devices from external threats. Businesses typically employ Cyber Security professionals to protect their confidential information, maintain employee productivity, and enhance customer confidence in products and services.

The world of Cyber Security revolves around the industry standard of confidentiality, integrity, and availability, or CIA. Privacy means data can be accessed only by authorized parties; integrity means information can be added, altered, or removed only by authorized users; and availability means systems, functions, and data must be available on-demand according to agreed-upon parameters.

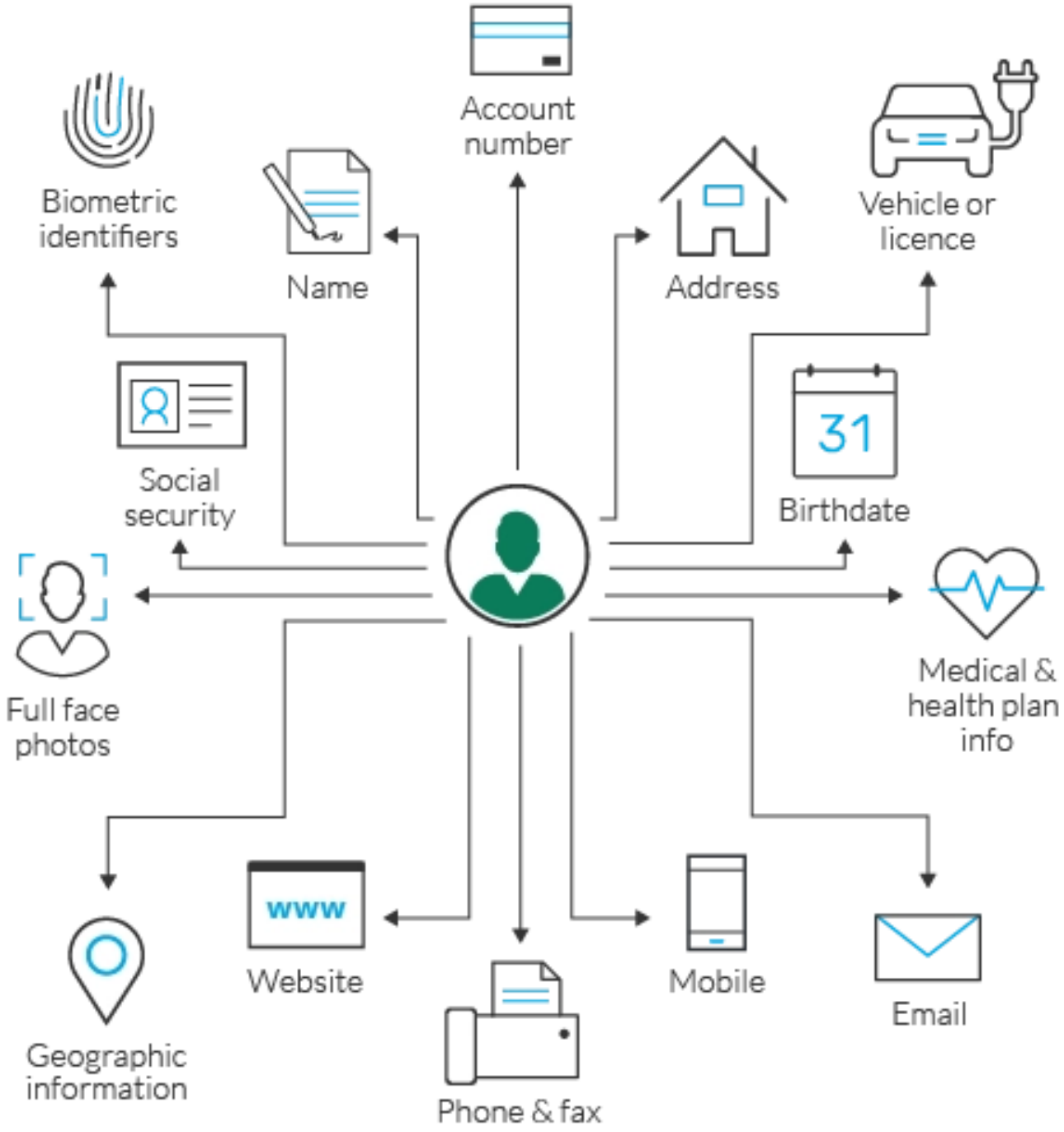
The main element of Cyber Security is the use of authentication mechanisms. For example, a user name identifies an account that a user wants to access, while a password is a mechanism that proves the user is who he claims to be.(1)

- Confidentiality is roughly equivalent to privacy. Confidentiality measures are designed to prevent sensitive information from unauthorized access attempts. It is common for data to be categorized according to the amount and type of damage that could be done if it fell into the wrong hands. More or less stringent measures can then be implemented according to those categories.
- Integrity involves maintaining the consistency, accuracy and trustworthiness of data over its entire lifecycle. Data must not be changed in transit, and steps must be taken to ensure data cannot be altered by unauthorized people (for example, in a breach of confidentiality).
- Availability means information should be consistently and readily accessible for authorized parties. This involves properly maintaining hardware and technical infrastructure and systems that hold and display the information. (2)

Best practices

- Keep software up-to-date
- Avoid opening suspicious emails
- Keep hardware up-to-date
- Use a secure file-sharing solution to encrypt data
- Use anti-virus and anti-malware
- Use a VPN to privatize your connections
- Check links before you click (3)

II. Personally Identifiable Information



(.)

Personally identifiable information (PII) is information that, when used alone or with other relevant data, can identify an individual.

PII may contain direct identifiers (e.g., passport information) that can identify a person uniquely, or quasi-identifiers (e.g., race) that can be combined with other quasi-identifiers (e.g., date of birth) to successfully recognize an individual.

Understanding Personally Identifiable Information

Advancing technology platforms have changed the way businesses operate, governments legislate, and individuals relate. With digital tools like cell phones, the Internet, e-commerce, and social media, there has been an explosion in the supply of all kinds of data.

Big data, as it is called, is being collected, analyzed, and processed by businesses and shared with other companies. The wealth of information provided by big data has enabled companies to gain insight into how to better interact with customers.

However, the emergence of big data has also increased the number of data breaches and cyberattacks by entities who realize the value of this information. As a result, concerns have been raised over how companies handle the sensitive information of their consumers. Regulatory bodies are seeking new laws to protect the data of consumers, while users are looking for more anonymous ways to stay digital.

Sensitive vs. Non-Sensitive Personally Identifiable Information

Sensitive PII

Personally identifiable information (PII) can be sensitive or non-sensitive. Sensitive personal information includes legal statistics such as:

- Full name
- Social Security Number (SSN)
- Driver’s license
- Mailing address
- Credit card information
- Passport information
- Financial information
- Medical records

Non-Sensitive PII

Non-sensitive or indirect PII is easily accessible from public sources like phonebooks, the Internet, and corporate directories. Examples of non-sensitive or indirect PII include:

- Zip code
- Race
- Gender
- Date of birth
- Place of birth
- Religion (4)

PII VERSUS PHI

Personally identifiable information encompasses any information that can be directly or indirectly linked to an individual's identity, according to the National Institute of Standards and Technology (NIST).

PII includes, but is not limited to, Social Security numbers, passport numbers, driver's license numbers, addresses, email addresses, photos, biometric data, or any other information that can be traced to one individual. Medical, educational, financial, and employment information all fall under PII.

The HIPAA Privacy Rule defines 18 identifiers that make health information PHI under HIPAA:

- Names
- All geographic subdivisions smaller than a state (street address, city, county, zip code)
- Dates, including birthdate, admission date, discharge date, and date of death
- Telephone numbers
- Fax numbers
- Email addresses
- Social Security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web URLs

- IP addresses
- Biometric identifiers; including fingerprints and voice
- Full face photos
- Any other unique identifying number, characteristic, or codes (5)

Tips for protecting Personally Identifiable Information :

- Use a complete security platform that can also protect your privacy
- Use a VPN
- Keep a close grip on your Social Security Number
- Protect your files
- Be on the lookout for phishing attacks
- Look for HTTPS when you browse
- Lock your devices (6)

III. Social Engineering

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Social engineering attacks happen in one or more steps. A perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack. Then, the attacker moves to gain the victim's trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources.

Social Engineering Attack Lifecycle

Social engineering attack techniques

- Baiting

The most reviled form of baiting uses physical media to disperse malware. For example, attackers leave the bait—typically malware-infected flash drives—in conspicuous areas where potential victims are certain to see them (e.g., bathrooms, elevators, the parking lot of a targeted company). The bait has an authentic look to it, such as a label presenting it as the company's payroll list.

- Scareware

A common scareware example is the legitimate-looking popup banners appearing in your browser while surfing the web, displaying such text such as, "Your computer may be infected with harmful spyware programs." It either offers to install the tool (often malware-infected) for you, or will direct you to a malicious site where your computer becomes infected.

- Pretexting

The attacker usually starts by establishing trust with their victim by impersonating co-workers, police, bank and tax officials, or other persons who have right-to-know authority. The pretexter asks questions that are ostensibly required to confirm the victim's identity, through which they gather important personal data.

- Phishing

An example is an email sent to users of an online service that alerts them of a policy violation requiring immediate action on their part, such as a required password change. It includes a link to an illegitimate website—nearly identical in appearance to its legitimate version—prompting the unsuspecting user to enter their current credentials and new password. Upon form submittal the information is sent to the attacker.

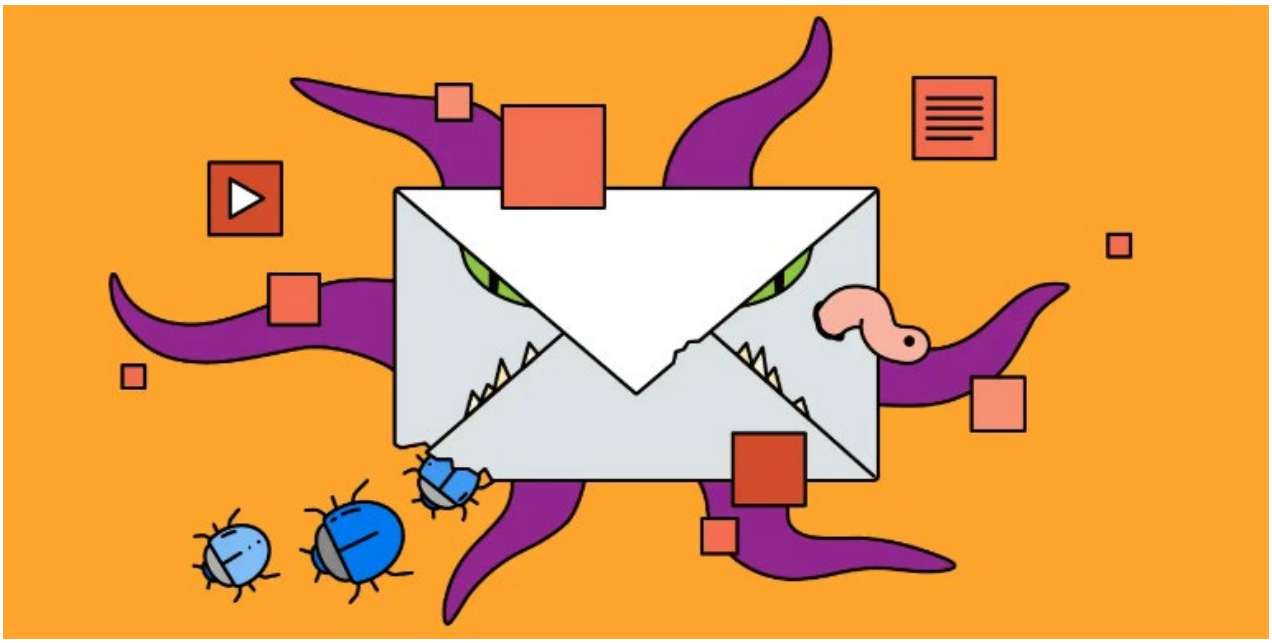
- Spear phishing

This is a more targeted version of the phishing scam whereby an attacker chooses specific individuals or enterprises. They then tailor their messages based on characteristics, job positions, and contacts belonging to their victims to make their attack less conspicuous. Spear phishing requires much more effort on behalf of the perpetrator and may take weeks and months to pull off. They're much harder to detect and have better success rates if done skillfully.

Social engineering prevention

- Don’t open emails and attachments from suspicious sources
- Use multifactor authentication
- Be wary of tempting offers
- Keep your antivirus/antimalware software updated (7)

IV. Email Links and Attachments



(.)

Email scams and viruses are nothing new—threats like phishing emails and malware have been around since the days when services like AOL still dominated the internet and email landscape. However, while technology has made a firm pivot away from the days of dial-up modems and service-hosted platforms, email remains the method of choice for hackers looking to use ransomware or other malicious software to effectively monetize their exploits or to simply cause harm.

If an attacker manages to get an employee to download and open a malicious file sent as an email attachment, the door will be opened for a variety of incredibly damaging scenarios for your business: data theft, fraudulent wire transfers, and leaking of confidential information are just a few of the possibilities. Given what's at stake, it's not an overstatement to say that email security is more important than ever.

Although it may be tempting to simply ask what types of email attachments are generally safe to open, the answer isn't so straightforward.

Common warning signs of an email that may harbor a malicious threat :

- Filenames with Double Extensions

Giving a misleading filename to an email attachment is not a new tactic by any means, but you'd be surprised how often hackers continue to get away with it. This can be as simple as adding what appears to be a harmless file type extension just before the actual extension with hopes of the potential victim overlooking it with a cursory glance.

- Suspicious Sender Addresses

Another favorite tactic from hackers involves masking their email addresses with fake ones that appear to be official. This can be in the form of a first and last name, or the name of a company, such as Facebook. However, when you click on the sender's details, you'll see the sender's address is something entirely different. Fake sender address emails are notorious for encouraging recipients to click on a link or download a supposedly safe attachment.

- Unwanted Offers

Sometimes a fake offer in the form of a deal or giveaway from what appears to be a well-known company can make it past your email host's spam filters. These emails typically have links that redirect you to a fake website that attempts to lure you into submitting your login credentials. However, some still come with email attachments containing misleading names.

Common preventions :

- Email Filtering

Your organization should have robust email filtering systems that can scan and categorize inbound and outbound email traffic. The filters should be able to either block or reroute spam emails to a separate inbox and away from the primary inbox.

- Email Firewalls

Before an email can be filtered, it must first be able to pass through a firewall. Email firewalls can scan emails for viruses and malware and prevent them from reaching an employee's inbox. They can also scan inbound emails associated with multiple accounts using different domain names and provide customization tools that enable IT teams to block certain domains while allowing others to pass through. Email firewalls are essential for catching and blocking emails containing threats like ransomware before they arrive in an inbox.

- Phishing Tests

Not even the best firewalls and filters are guaranteed to block every potential malicious email that may find its way to your organization. Employee education and adherence to best practices are also a significant part of the equation. One highly effective tool you should be leveraging for email security is phish testing. (8)

V. Online Security Basics

(.)

WHAT IS ONLINE SECURITY?

Online security is something most of us use on a daily basis – sometimes we don't even know we are using it! It is commonly used by websites to keep your personal information as safe as possible. Some websites apply their security by asking for your email address and other contact details which are unique to you. Most websites will have a disclaimer explaining exactly how the information you provide will be used and/or distributed. This should be reviewed carefully to ensure you are fully aware of your digital footprint and how your personal data is being stored and used.

Although most websites and platforms do everything that they can to prevent your information from unauthorized access – the connected and open nature of the internet means that no security system can be 100% secure.

WHAT IS A DIGITAL FOOTPRINT?

A digital footprint is like a file of unique, traceable online activities, contributions, communications and actions specific to you. When you supply information to a website, sign up for a social media account or contribute to a forum, these activities will automatically become part of your personal digital footprint.

Our 'digital footprints' or online identities are broken down into two categories. One being our active digital footprints, which is made up of websites and platforms that we have purposely given information to – such as when you sign up for a social media account. The other is called our passive digital footprint – where our data is collected without us knowing. This is used by businesses and websites in order to track website traffic and is collected automatically. This data is commonly referred to as 'cookies' and gets stored while you are browsing a particular webpage.

DIFFERENT TYPES OF ONLINE SECURITY

Almost all of us use online security on a daily basis. Some examples of frequently used online security include:

- Complex password entry – Social media platforms and websites that allow you to have an account or offer a login entry system will more often than not, ask you to create a password in order to gain access in the future. Because of advancements in technology and the sophistication of hacking software – websites are asking for passwords to be increasingly complex. They often require a combination of at least 8 characters made up of one uppercase letter, a number and at least one special symbol such as a question mark or full stop.
- Security questions – Commonly, banks will ask you to set up security questions. These questions will be personal to you and you should never share your answers with anybody. Your bank may ask you to enter the answers to these questions when logging in every time or if they recognize that you are trying to log in from a different location than usual. Over recent years, some social media

platforms have also started using security questions as a method of identifying users.

- Anti-virus software/freeware – Antivirus software that can be purchased or freely downloaded can be very useful in providing protection to internet users. Most security products will block viruses and threats from accessing or affecting your device – good quality security products offer a scanning facility to check your device and remove any malware in the process. Always consider the strength of your firewall along with a good antivirus program to get the best results and to keep your personal information as secure as possible.
- Two-factor authentication – Increasingly, companies and social media platforms are offering two-factor authentication, which is considered a "second layer" of security online. Two factor authentication means that more than just a username and password are required when logging in to an account. Most companies and social media platforms do this by sending a unique code to the user via SMS. This code will expire after a certain amount of time and also lets people know if anyone is attempting to gain access to their account without permission.

The types of online security listed above are just a fraction of the layers that online security plays in all of our lives each day.

THREATS TO INTERNET SAFETY

Regardless of the volume and effectiveness of online security that we use to protect ourselves, we are never 100% safe from online threats. Some of the more commonly seen threats include:

- Botnets – Botnets are networks of multiple computers that can coordinate specific tasks which are often repetitive to help maintain websites and chatrooms. These networks can be hijacked and controlled without a user's knowledge, spreading different kinds of malware and sending high volumes of emails containing spam and viruses to inboxes around the world.
- Hacking – Hackers gain unauthorized access to your device through a number of ways. Once they have gained access to your device they are then able to access your personal information or any other person's information you store on the system.
- Pharming – Pharming is when someone is able to redirect anyone using the URL of a secure, legitimate website to a fake site. They are able to do this even if the URL of the victim website is typed correctly.
- Phishing – Phishing is the use of fake emails, websites and text messages made to look like they are from an authentic company with the purpose of stealing personal information about you.
- Malware – Malware is malicious software that cyber criminals can place on your device. It is one of the most common ways in which your device can be infected and once it has been applied, it can be used to alter/delete files, send emails on

your behalf, intimidate people and reformat your hard drive so you lose all of your information or are unable to access it.

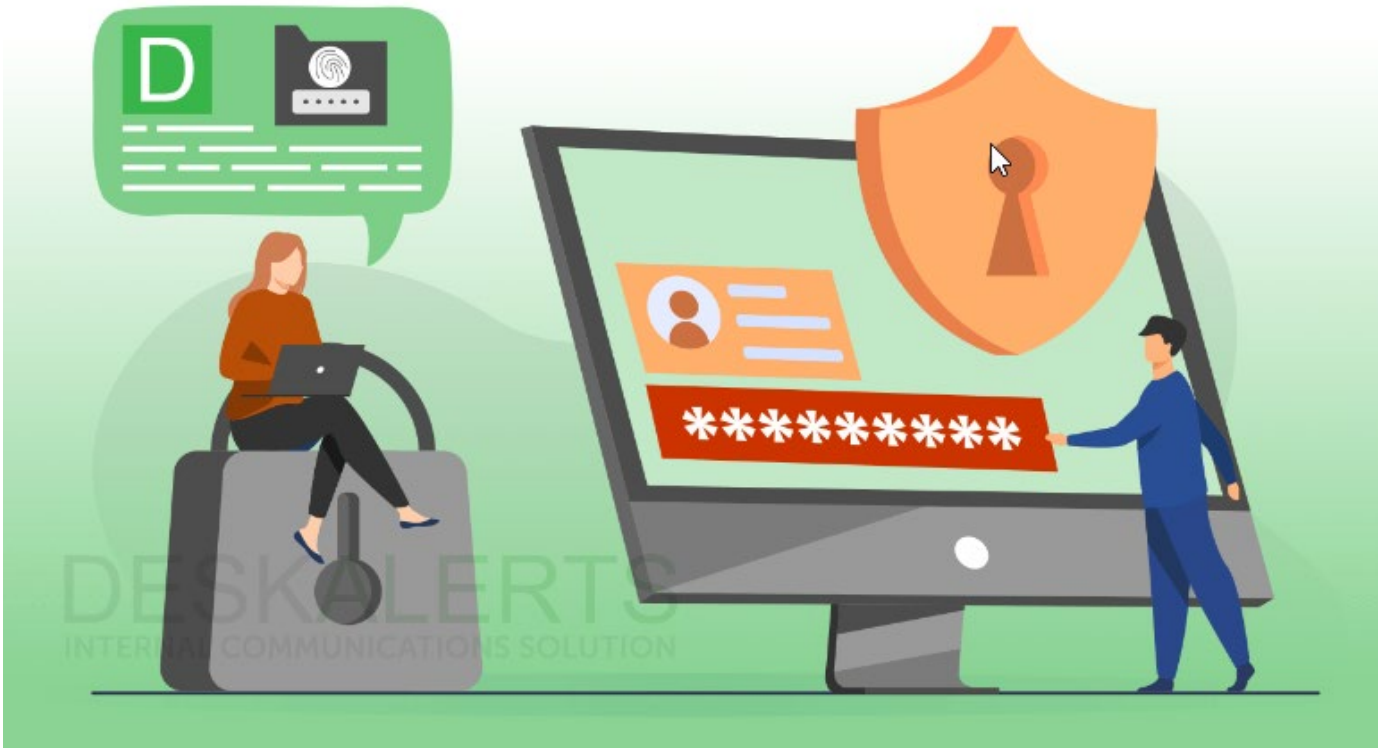
- Trojan horses – Trojan Horses are one of the least commonly detected and most dangerous forms of security threat. A Trojan horse is a malicious file embedded or disguised within authentic software and will run automatically. Once the file is running, not only can it record your keystrokes and delete your files but it can also use your computer to hack others and spy on you through your webcam.
- Spyware – Spyware is often used by cyber criminals but can also be used by people in authority if they suspect that someone is engaging in illegal activity. It goes completely undetected by the recipient and if someone is applying it maliciously, it can be difficult to remove once it has been activated on an infected computer.
- Ransomware – Ransomware is a form of malware which restricts access to the infected device(s) until they (the perpetrator) release the lock. In most cases of ransomware, cybercriminals demand payment from the victim in order to remove the restriction.

ONLINE SAFETY TIPS

Although we can never be totally safe from attacks and security breaches online, there are things that we can do to reduce our chances of being targeted. The following tips will help you to stay as safe as possible online:

- Use strong passwords – We cannot emphasize enough how important it is to use complex passwords. Use a system to create strong and memorable passwords and change them regularly.
- Enable multi-factor authentication – Two-factor or multi-factor authentication adds another level to your personal security online. The more layers the better!
- Make sure your network is secure – Remember that public Wi-Fi is often unsecured, leaving your device and information vulnerable to hackers.
- Make sure you use a firewall – Even on secure networks, you should still use a firewall.
- Protect your identity – Don’t share personal information publicly. The less information that is ‘out there’ the safer you are. Sharing is not always for caring!
- Be scam aware – Check all emails carefully before clicking on any links or opening any files.
- Do necessary updates – It can be annoying to keep updating devices and software but they often contain critical security updates. Better safe than sorry! (9)

VI. Computer Best Practices



(.)

Here are some information about how to securely use your computer in general :

- **Keep Mobile devices and laptops safe**
    - When leaving your computer, lock the screen with a password to safeguard the data on your computer. Also, always lock your doors when leaving the computer unattended.
    - Never leave your devices or laptop in the car. It's a best practice to keep work laptops and devices on your person at all times while on the road. The trunk of your car is not any safer. There may be criminals watching to take advantage of this situation.
- **Don't allow family members to use your work devices.**
    - If you think of your laptop and mobile devices as work-only assets, it makes it easier to control access to sensitive data. For remote workers, treat your work laptop, mobile device and sensitive data as if you were sitting in a physical office location. This will help you continuously associate your actions with a security-first and data-aware mentality in

mind. For example, in a physical office location, your child wouldn't be able to use your work mobile device for games or movies.

- **Invest in an antivirus software.**
    - If you use your personal laptop for work, it's important to keep your system protected. Scan all attachments that are sent to you. Viruses can lurk in emails from friends and family. If you receive a link in an email from a trusted source, hover over the link using your mouse and look in the bottom bar of your web browser to reveal the true URL and validate that the link is legitimate. This will ensure that you know where you are going on the Internet, and whether or not you want to go there.
- **Keep your computer with all the software updated.**
    - It is essential the use anti-virus software. Most anti-virus software gives the user the ability to do automatic updates.
    - Ensure that your operating system (e.g W10/OS X) is continuously updated and patched. It is also important to keep other software on your computer updated. Software updates often include essential bug fixes and security features that address existing vulnerabilities.
    - Make sure that the firewall on your computer is enabled. This will help to keep unauthorized people from snooping around your computer when it's connected to the Internet.
- **Keep Work Data on Work Computers.**
    - Introducing a personal computer to a work network, even remotely, put that networks at risk, and yourself at risk, accepting the potential liability of extensive damages though violations of policy, practices or both. Use remote environment such as Office 365, so you could work online and avoid downloading or synching files or emails to a personal device.
- **Minimize storage of sensitive information.**
    - Delete sensitive information whenever you can. Keep it off of your workstation, laptop computer, and other electronic devices if at all possible.
    - Don't keep sensitive information or your only copy of critical data, projects, files, etc. on portable or mobile devices (such as laptop computers, tablets, phones, memory sticks, CDs/DVDs, etc.) unless they are properly protected. These items are extra vulnerable to theft or loss.
- **Avoid public Wi-Fi; if necessary, use personal hotspots or some way to encrypt your web connection.**
    - Public Wi-Fi introduces significant security risk and should be avoided if possible. If you need to access the internet from a public Wi-Fi location, you have two essential problems to solve. First, other people have access to that network and, without a firewall between you and them, threat actors can pound away at your computer from across the room. Second, any interested observers on either the current network or any other public networks your data hits between you and your workplace can monitor your

traffic as it goes by. It is important to find a way to protect your PC and encrypt your traffic.
    - For some use cases, you can also set up encrypted remote connections into a remote desktop or other individual server. Many of these connection types (RDP, HTTPS, SSH) include encryption as part of their service direction and do not require an additional VPN or other encryption service to secure the data in-transit.
    - One option is to use a personal hotspot from a dedicated device or your phone. Using a hot spot does eliminate the problem of getting hacked by people on the same public Wi-Fi.
    - For many remote access applications, you should use a VPN. VPNs provide a flexible connection to connect to different services (web pages, email, a SQL server, etc.) and can protect your traffic. Keep in mind that VPN services provided for privacy purposes only protect the data to and from the VPN provider, not to the destination so are not suitable for protecting remote access.
- **Avoid surfing websites that you don't already know**
    - Browsers are quickly becoming one of the larger vulnerabilities in computing. Adware and spyware are written specifically to exploit Chrome, Internet Explorer and Firefox. So try and stick with the websites you trust.
- **Only Download files legally**.
    - Along with the possibility of significant legal penalties, downloading files from peer-to-peer networks can be harmful to your machine. These downloaded files are sometimes riddled with viruses and spyware.
- **Keep personal information safe**.
    - Reduce your risk of identity theft. Never share your personal information via email, no matter how official the email looks. Official business that requires personal information should not happen via unsecured email.
    - Also, limit information on social media sites. For many people, birth dates, anniversaries, addresses, phone numbers, and a lot of other personal information can be found on social media sites. Protect yourself from identity theft and other scams by limiting what information you disclose online and who can see that information. (10)

VII. Network Security

How does network security work?

Network security combines multiple layers of defenses at the edge and in the network. Each network security layer implements policies and controls. Authorized users gain access to network resources, but malicious actors are blocked from carrying out exploits and threats.

How do I benefit from network security?

Digitization has transformed our world. How we live, work, play, and learn have all changed. Every organization that wants to deliver the services that customers and employees demand must protect its network. Network security also helps you protect proprietary information from attack. Ultimately it protects your reputation.

Types of network security

- Firewalls

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

- Intrusion prevention systems

An intrusion prevention system (IPS) scans network traffic to actively block attacks. Secure IPS appliances do this by correlating huge amounts of global threat intelligence

to not only block malicious activity but also track the progression of suspect files and malware across the network to prevent the spread of outbreaks and reinfection.

- Workload security

Workload security protects workloads moving across different cloud and hybrid environments. These distributed workloads have larger attack surfaces, which must be secured without affecting the agility of the business.

- Network segmentation

Software-defined segmentation puts network traffic into different classifications and makes enforcing security policies easier. Ideally, the classifications are based on endpoint identity, not mere IP addresses. You can assign access rights based on role, location, and more so that the right level of access is given to the right people and suspicious devices are contained and remediated.

- VPN

A virtual private network encrypts the connection from an endpoint to a network, often over the internet. Typically, a remote-access VPN uses IPsec or Secure Sockets Layer to authenticate the communication between device and network.

- Access control

Not every user should have access to your network. To keep out potential attackers, you need to recognize each user and each device. Then you can enforce your security policies. You can block noncompliant endpoint devices or give them only limited access. This process is network access control (NAC).

- Anti-virus and anti-malware software

"Malware," short for "malicious software," includes viruses, worms, Trojans, ransomware, and spyware. Sometimes malware will infect a network but lie dormant for days or even weeks. The best antimalware programs not only scan for malware upon entry, but also continuously track files afterward to find anomalies, remove malware, and fix damage.

- Application security

Any software you use to run your business needs to be protected, whether your IT staff builds it or whether you buy it. Unfortunately, any application may contain holes, or vulnerabilities, that attackers can use to infiltrate your network. Application security encompasses the hardware, software, and processes you use to close those holes.

- Behavioral analytics

To detect abnormal network behavior, you must know what normal behavior looks like. Behavioral analytics tools automatically discern activities that deviate from the norm. Your security team can then better identify indicators of compromise that pose a potential problem and quickly remediate threats.

- Cloud security

Cloud security is a broad set of technologies, policies, and applications applied to defend online IP, services, applications, and other imperative data. It helps you better manage your security by shielding users against threats anywhere they access the internet and securing your data and applications in the cloud.

- Data loss prevention

Organizations must make sure that their staff does not send sensitive information outside the network. Data loss prevention, or DLP, technologies can stop people from uploading, forwarding, or even printing critical information in an unsafe manner.

- Email security

Email gateways are the number one threat vector for a security breach. Attackers use personal information and social engineering tactics to build sophisticated phishing campaigns to deceive recipients and send them to sites serving up malware. An email security application blocks incoming attacks and controls outbound messages to prevent the loss of sensitive data.

- Industrial network security

As you are digitizing your industrial operations, the deeper integration between IT, cloud, and industrial networks is exposing your Industrial Control Systems (ICS) to cyberthreats. You need full visibility into your OT security posture to segment the industrial network, and feed IT security tools with rich details on OT devices and behaviors.

- Mobile device security

Cybercriminals are increasingly targeting mobile devices and apps. Within the next three years, 90 percent of IT organizations may support corporate applications on personal mobile devices. Of course, you need to control which devices can access your network. You will also need to configure their connections to keep network traffic private.

- Security information and event management

SIEM products pull together the information that your security staff needs to identify and respond to threats. These products come in various forms, including physical and virtual appliances and server software.

- Web security

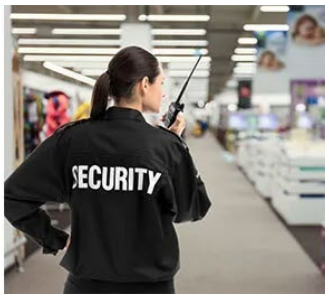
A web security solution will control your staff's web use, block web-based threats, and deny access to malicious websites. It will protect your web gateway on site or in the cloud. "Web security" also refers to the steps you take to protect your own website.

- Wireless security

Wireless networks are not as secure as wired ones. Without stringent security measures, installing a wireless LAN can be like putting Ethernet ports everywhere, including the parking lot. To prevent an exploit from taking hold, you need products specifically designed to protect a wireless network. (11)

VIII. Physical Security



The modern business owner faces security risks at every turn. As technology continues to advance, threats can come from just about anywhere, and the importance of physical security has never been greater. While many companies focus their prevention efforts on cybersecurity and hacking, physical threats shouldn't be ignored. Every breach, big or small, impacts your business, from financial losses, to damaged reputation, to your employees feeling insecure at the office. Even for small businesses, having the right physical security measures in place can make all the difference in keeping your business, and your data, safe.

What is physical security?

Let's start with a physical security definition, before diving into the various components and planning elements. Physical security measures are designed to protect buildings, and safeguard the equipment inside. In short, they keep unwanted people out, and give access to authorized individuals. While network and cybersecurity are important,

preventing physical security breaches and threats is key to keeping your technology and data safe, as well as any staff or faculty that have access to the building. Without physical security plans in place, your office or building is left open to criminal activity, and liable for types of physical security threats including theft, vandalism, fraud, and even accidents.

In the built environment, we often think of physical security control examples like locks, gates, and guards. While these are effective, there are many additional and often forgotten layers to physical security for offices that can help keep all your assets protected. A comprehensive physical security plan combines both technology and specialized hardware, and should include countermeasures against intrusion such as:

- Site design and layout
- Environmental components
- Emergency response readiness
- Training
- Access control
- Intrusion detection
- Power and fire protection

From landscaping elements and natural surveillance, to encrypted keycards or mobile credentials, to lockdown capabilities and emergency mustering, there are many different components to preventing all different types of physical security threats in the modern workplace. You can use a Security Audit Checklist to ensure your physical security for buildings has all the necessary components to keep your facility protected from threats, intrusions and breaches.

Before updating a physical security system, it's important to understand the different roles technology and barriers play in your strategy. The smartest security strategies take a layered approach, adding physical security controls in addition to cybersecurity policies. This means building a complete system with strong physical security components to protect against the leading threats to your organization.

The four main security technology components are:

- Deterrence – These are the physical security measures that keep people out or away from the space. Deterrent security components can be a physical barrier, such as a wall, door, or turnstyle. Technology can also fall into this category. Access control systems and video security cameras deter unauthorized individuals from attempting to access the building, too.
- Detection – Just because you have deterrents in place, doesn't mean you're fully protected. Detection components of your physical security system help identify a

potential security event or intruder. Sensors, alarms, and automatic notifications are all examples of physical security detection.

- Delay – There are certain security systems that are designed to slow intruders down as they attempt to enter a facility or building. Access control, such as requiring a key card or mobile credential, is one method of delay. Smart physical security strategies have multiple ways to delay intruders, which makes it easier to mitigate a breach before too much damage is caused.
- Response – These are the components that are in place once a breach or intrusion occurs. Examples of physical security response include communication systems, building lockdowns, and contacting emergency services or first responders.
- Together, these physical security components work to stop unwanted individuals from accessing spaces they shouldn't, and notify the necessary teams to respond quickly and appropriately. Your physical security plans should address each of the components above, detailing the technology and processes you'll use to ensure total protection and safety.

How do physical security policies impact cybersecurity and data protection?

Today's security systems are smarter than ever, with IoT paving the way for connected and integrated technology across organizations. However, cloud-based platforms, remote and distributed workforces, and mobile technology also bring increased risk. In fact, 97% of IT leaders are concerned about a data breach in their organization. But cybersecurity on its own isn't enough to protect an organization. That's why a complete physical security plan also takes cybersecurity into consideration.

Cyber and physical converged security merges these two disparate systems and teams for a holistic approach to security. Even with stringent cybersecurity practices, like encryption and IP restrictions, physical security failures could leave your organization vulnerable. Gaps in physical security policies, such as weak credentials or limited monitoring capabilities, make it easier for people to gain access to data and confidential information.

Take a look at these physical security examples to see how the right policies can prevent common threats and vulnerabilities in your organization.

- Restrict access to IT and server rooms, and anywhere laptops or computers are left unattended
- Use highly secure access credentials that are difficult to clone, fully trackable, and unique to each individual
- Require multi-factor authentication (MFA) to unlock a door or access the building

- Structure permissions to employ least-privilege access throughout the physical infrastructure
- Eliminate redundancies across teams and processes for faster incident response
- Integrate all building and security systems for a more complete view of security and data trends
- Set up automated security alerts to monitor and identify suspicious activity in real-time

Most common threats to physical security

While your security systems should protect you from the unique risks of your space or building, there are also common physical security threats and vulnerabilities to consider. The top 5 most common threats your physical security system should protect against are:

- Theft and burglary
- Vandalism
- Natural disasters
- Terrorism or sabotage
- Violence in the workplace

Depending on where your building is located, and what type of industry you're in, some of these threats may be more important for you to consider. For example, if your building or workplace is in a busy public area, vandalism and theft are more likely to occur. If your building houses a government agency or large data storage servers, terrorism may be higher on your list of concerns.

The above common physical security threats are often thought of as outside risks. However, internal risks are equally important. Human error is actually the leading cause of security breaches, accounting for approximately 88% of incidents, according to a Stanford University study. Some of the factors that lead to internal vulnerabilities and physical security failures include:

- Employees sharing their credentials with others
- Accidental release or sharing of confidential data and information
- Tailgating incidents with unauthorized individuals
- Easily hacked authentication processes
- Slow and limited response to security incidents

Benefits of physical security technology

- Prevent unauthorized entry — Providing a secure office space is the key to a successful business. Nearly one third of workers don't feel safe at work, which can take a toll on productivity and office morale. Providing security for your customers is equally important. Not only should your customers feel secure, but their data must also be securely stored. Data breaches compromise the trust that your business has worked so hard to establish. Implementing a rigorous commercial access control system as part of your physical security plans will allow you to secure your property from unauthorized access, keeping your assets and employees safe and preventing damage or loss.
- Proactive intrusion detection — As the first line of defense for your building, the importance of physical security in preventing intrusion cannot be understated. Installing a best-in-class access control system ensures that you'll know who enters your facility and when. With an easy-to-install system like Openpath, your intrusion detection system can be up-and-running with minimal downtime. Plus, the cloud-based software gives you the advantage of viewing real-time activity from anywhere, and receiving entry alerts for types of physical security threats like a door being left ajar, an unauthorized entry attempt, a forced entry, and more. With Openpath's unique lockdown feature, you can instantly trigger a full system lockdown remotely, so you take care of emergencies quickly and efficiently. Cloud-based and mobile access control systems offer more proactive physical security measures for your office or building.
- Scalable physical security implementation — With data stored on the cloud, there is no need for onsite servers and hardware that are both costly and vulnerable to attack. Cloud-based physical security control systems can integrate with your existing platforms and software, which means no interruption to your workflow. Both for small businesses experiencing exponential growth, and for enterprise businesses with many sites and locations to consider, a scalable solution that's easy to install and quick to set up will ensure a smooth transition to a new physical security system. Cloud-based systems are naturally more flexible compared to legacy systems, which makes it easier to add or remove entries, install new hardware, or implement the system across new building locations.
- Seamless system integrations — Another benefit of physical security systems that operate in the cloud is the ability to integrate with other software, applications, and systems. While a great access control system is essential to any physical security plan, having the ability to connect to other security tools strengthens your entire security protocol. For example, Openpath's access control features an open API, making it quick and easy to integrate with video surveillance and security cameras, user management systems, and the other tools you need to run your business.
- Audit trails and analytics — One of the benefits of physical security control systems is that the added detection methods usually include reporting and audit trails of the activity in your building. This data is crucial to your overall security. Being able to easily and quickly detect possible weaknesses in your system

enables you to implement new physical security plans to cover any vulnerable areas. In the event that you do experience a breach, having detailed reports will provide necessary evidence for law enforcement, and help you identify the culprit quickly. Analytics on the performance of your physical security measures allow you to be proactive in finding efficiencies, enabling better management and lessening the burden on your HR and IT teams. (12)

IX. Mobile Device Security

What is Mobile Device Security?

Mobile Device Security refers to the measures designed to protect sensitive information stored on and transmitted by laptops, smartphones, tablets, wearables, and other portable devices. At the root of mobile device security is the goal of keeping unauthorized users from accessing the enterprise network. It is one aspect of a complete enterprise security plan.

Why is Mobile Device Security important?

With more than half of business PCs now mobile, portable devices present distinct challenges to network security, which must account for all of the locations and uses that employees require of the company network. Potential threats to devices include malicious mobile apps, phishing scams, data leakage, spyware, and unsecure Wi-Fi networks. On top of that, enterprises have to account for the possibility of an employee losing a mobile device or the device being stolen. To avoid a security breach, companies should take clear, preventative steps to reduce the risk.

What are the benefits of Mobile Device Security?

Mobile device security, or mobile device management, provides the following:

- Regulatory compliance
- Security policy enforcement
- Support of “bring your own device” (BYOD)
- Remote control of device updates
- Application control
- Automated device registration
- Data backup

Above all, mobile device security protects an enterprise from unknown or malicious outsiders being able to access sensitive company data.

How does Mobile Device Security work?

Securing mobile devices requires a multi-layered approach and investment in enterprise solutions. While there are key elements to mobile device security, each organization needs to find what best fits its network.

To get started, here are some mobile security best practices:

- Establish, share, and enforce clear policies and processes

Mobile device rules are only as effective as a company's ability to properly communicate those policies to employees. Mobile device security should include clear rules about:

- What devices can be used
- Allowed OS levels
- What the company can and cannot access on a personal phone
- Whether IT can remote wipe a device
- Password requirements and frequency for updating passwords
- Password protection

One of the most basic ways to prevent unauthorized access to a mobile device is to create a strong password, and yet weak passwords are still a persistent problem that contributes to the majority of data hacks. Another common security problem is workers using the same password for their mobile device, email, and every work-related account. It is critical that employees create strong, unique passwords (of at least eight characters) and create different passwords for different accounts.

- Leverage biometrics

Instead of relying on traditional methods of mobile access security, such as passwords, some companies are looking to biometrics as a safer alternative. Biometric authentication is when a computer uses measurable biological characteristics, such as face, fingerprint, voice, or iris recognition for identification and access. Multiple biometric authentication methods are now available on smartphones and are easy for workers to set up and use.

- Avoid public Wi-Fi

A mobile device is only as secure as the network through which it transmits data. Companies need to educate employees about the dangers of using public Wi-Fi networks, which are vulnerable to attacks from hackers who can easily breach a device,

access the network, and steal data. The best defense is to encourage smart user behavior and prohibit the use of open Wi-Fi networks, no matter the convenience.

- Beware of apps

Malicious apps are some of the fastest growing threats to mobile devices. When an employee unknowingly downloads one, either for work or personal reasons, it provides unauthorized access to the company's network and data. To combat this rising threat, companies have two options: instruct employees about the dangers of downloading unapproved apps, or ban employees from downloading certain apps on their phones altogether.

- Mobile device encryption:

Most mobile devices are bundled with a built-in encryption feature. Users need to locate this feature on their device and enter a password to encrypt their device. With this method, data is converted into a code that can only be accessed by authorized users. This is important in case of theft, and it prevents unauthorized access.(13)

What is Bring Your Own Device?

Bring your Own Device (BYOD) is the set of policies in a business that allows employees to use their own devices – phone, laptop, tablet or whatever – to access business applications and data, rather than forcing employees to use company-provided devices for that purpose.

BYOD also refers to the ability to bring one's own mobile phone to a new carrier, but this article will focus only on the first definition as it applies to IT organizations.

BYOD has made a huge impact in organizations, and research indicates that nearly 80 percent of all organizations support BYOD personal devices today, while another survey found that about 95 percent of employees state they use at least one BYOD device for work functions.

What are the benefits of BYOD?

Some of the many BYOD benefits include

- Productivity gains by employees
- Improved morale and convenience
- Easier to attract new hires compared to non-BYOD companies
- Company cost savings

- Higher job satisfaction
- Reduce the number of smartphones employees need to carry
- Better overall user experience since employees typically know how to use their own devices

Why is BYOD important?

The consumerization of IT has had far-reaching impact. Employees increasingly desire to utilize their favored devices – whether Mac, PC laptop, iPhone, Android, or whatever else may come. As a result, enterprises have created mobile applications which often enable simple and better-to-manage solutions in many instances for business owners. There are a number of reasons why BYOD is important, including:

- Improved employee productivity. Employees who have the ability to use a favored, familiar device are likely to be more productive than those who are forced to learn the ins and outs of unfamiliar equipment. More importantly, employees find it easier to work from home or other locations when they do not have to switch devices.
- Device cost savings. More BYOD translates to fewer company assets to issue, track, manage, repair, upgrade, and maintain.
- Simplified onboarding and offboarding. BYOD MDM tools can enable or disable company network access without the need to modify the BYOD device.
- Better employee relations. Employees with BYOD devices feel more in control of their environment, are often more productive when they feel empowered with BYOD and are more apt to work remotely when they can use the same device.
- BYOD as perk. For many employees, BYOD demonstrates the company is forward-thinking and tech-savvy. Most employees receive some reimbursement for using their BYOD devices, since organizations see substantial savings by not having to purchase and maintain those devices.

How does BYOD work?

There are a number of modes of BYOD operation. First, the organization should establish security policies for every device since weak passwords and unsecured devices can lead to data loss. BYOD polices should establish:

- Minimum security controls including data encryption and password strength
- What type of enterprise data can be stored on local devices (if any)
- Whether timeout controls and auto-lock features will be enforced
- Which mobile device security or mobile data management (MDM) software must be installed on BYOD devices, if any.
- Whether the organization is authorized to remotely wipe the device of business information if lost, if employment is terminated, or if a policy breach is detected

A business' level of security procedures will depend on the type of organization; for example finance or healthcare organizations require higher levels of security than a small start-up web design firm.Once security policies are established, organizations should define acceptable usage guidelines to determine how BYOD devices may be used during the course of business activities. This will help prevent malware or viruses from gaining access through unsecured websites and applications. These policies should cover

- Acceptable applications for employees to access from personal devices, with a clear delineation of the types of applications acceptable – and those that are not.
- Which websites are off-limits while connected to enterprise resources, corporate network or VPN.
- Which enterprise applications and data can be accessed from user devices; i.e. email, calendar, messaging, contacts, etc.
- Storing and transmission of illicit material, or utilizing devices for other outside business activities from personal devices

Polices should be enforced through the use of BYOD MDM software, which enables monitoring, managing, and configuring BYOD and employer-owned devices from a single central dashboard. Typical MDM functionality for BYOD includes

- Automatic scans of BYOD devices for threats, including blocking dangerous applications from the corporate network
- Pushing anti-malware updates to devices and ensuring its installation
- Remote installation of updates and patches to OS and applications
- Security policy enforcement
- Automatic backup of enterprise applications and data periodically or on demand
- Wiping lost, stolen, or compromised devices remotely

Once BYOD policies are established, they must be communicated to employees and sufficient training provided to make adoption simple and widespread. A training manual for new hires that outlines the policies and why they were chosen can help alleviate fears of the organization 'spying' on employees and help increase their comfort level with polices and MDM software alike. This should conclude with every BYOD employee agreeing that they have read and understood these policies to protect the organization from any liability caused by illegal or inappropriate use of their devices.

Finally, BYOD plans should include an exit plan for employees who leave, regardless of their reason for departure. This should include HR and network directory exit plan and should have a BYOD exit checklist that includes disabling of company email accounts,

remotely wiping employer information from devices and entirely wiping company issued devices and changing any shared password to company accounts.

Additionally, BYOD policies could include defining a stipend from the company to help pay for BYOD data plans or home broadband connectivity, and whether employees who check email or answer business calls after hours are entitled to overcome compensation.

What are the risks of BYOD?

Although the benefits of BYOD are many, there are significant risks to the organization. Businesses must define and deploy security policies and measures to prevent or repair security holes to prevent the exfiltration of intellectual property or protected information. An IDG survey found that over half of all senior IT security and technology professionals reported that serious violations of personal mobile device use occurred in their organizations.

Since BYOD devices connect both to sensitive corporate applications and potentially risky networks and services, the risk of malware infection or data exfiltration is high. Loss of a BYOD device could lead to third parties accessing unsecured data or applications, and even an employee who leaves the company can put enterprise data at risk if the sensitive information is not deleted or applications wiped from the BYOD device. Other risks include devices that are shared by family members, devices that are sold while still retaining sensitive information, or devices compromised by an employee visit to an infected website. Even the use of public hotspots presents a security risk.

Organizations must ensure that all applications and OS versions on BYOD devices are up-to-date since malware threats often target recently uncovered vulnerabilities. Businesses must have the agility to support a broad range of devices, which can put a large burden on the IT organization, which can be addressed by outsourcing MDM to an organization focused on ensuring BYOD security. Some of these challenges can be addressed by containerization and app virtualization, which packages enterprise applications and streams them to BYOD devices, ensuring that every employee has the most current version of a given application.

Another risk often overlooked is the simple determination of who ‘owns’ a phone number. This is a particular issue for salespeople or others in key customer-facing roles who may have become accustomed to reaching the business via an employee’s

personal mobile number. If a key salesperson leaves the organization for another job, those customers may potentially be calling a competitor when they think they are calling the organization.

What are the keys to effective BYOD?

Although there are many considerations for effective BYOD deployment, here are three key factors to help bring a plan into focus.

First, assess the current business and technology requirements for user devices. Gain an understanding of the mobile application requirements that will help employees do their jobs and determine what data need be accessed from mobile devices. Determine which applications are critical, which can currently provide secure information access, and which might be considered for replacement with newer, cloud-based or SaaS applications.

Next, decide if BYOD and MDM software will be delivered from on-premises servers, from a third-party service, or from the cloud.

Finally, draft a BYOD policy that business leaders and employees can agree to, as outlined at the beginning of this article. Adopting a policy and having employees sign on to the terms of that policy will help keep the organization’s applications and data safe while offering the employees the convenience of using their own devices for both business and personal access.(14)

References

1. https://www.simplilearn.com/introduction-to-cyber-security-article
2. https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA
3. https://www.titanfile.com/blog/cyber-security-tips-best-practices/
4. https://www.investopedia.com/terms/p/personally-identifiable-information-pii.asp
5. https://healthitsecurity.com/news/key-differences-between-phi-and-pii-how-they-impact-hipaa-compliance
6. https://www.mcafee.com/blogs/privacy-identity-protection/take-it-personally-ten-tips-for-protecting-your-personally-identifiable-information-pii/
7. https://www.imperva.com/learn/application-security/social-engineering-attack/
8. https://woodruffsawyer.com/cyber-liability/which-emails-are-safe/
9. https://www.cybersmile.org/what-we-do/advice-help/online-security
10. https://www.csusm.edu/iits/services/security/security-guidance/safe-computing.html
11. https://www.cisco.com/c/en/us/products/security/what-is-network-security.html
12. https://www.openpath.com/physical-security-guide
13. https://www.vmware.com/topics/glossary/content/mobile-device-security.html

14. https://www.vmware.com/topics/glossary/content/bring-your-own-device-byod.html