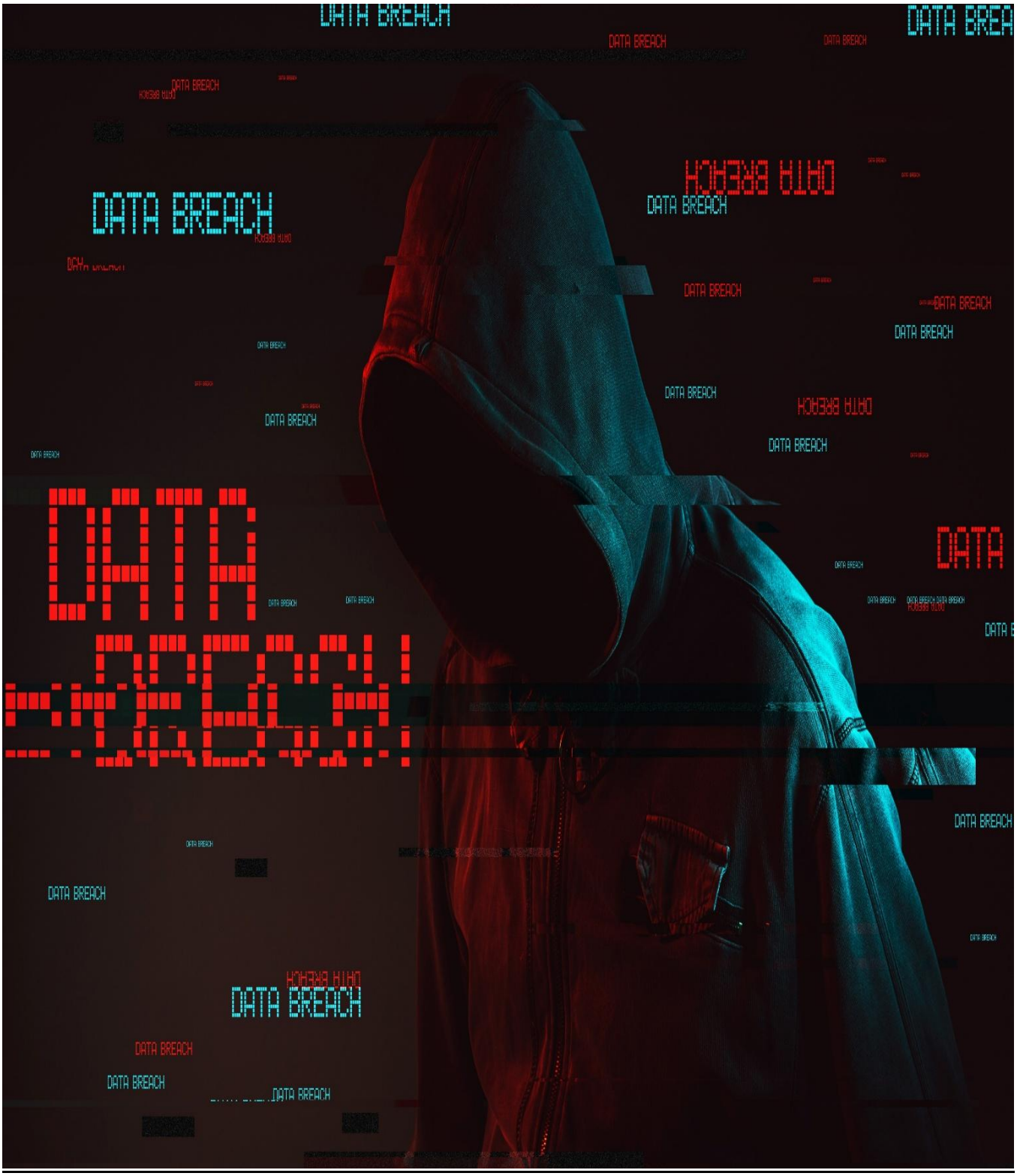
Al-Alamein international university

Introduction to emerging technologies



What is cybersecurity all about?

Cybersecurity is 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 through ransomware; or interrupting normal business processes. Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

A successful cybersecurity posture has multiple layers of protection spread across the computers, networks, programs, or data that one intends to keep safe. In an organization, a unified threat management gateway system can automate integrations across products and accelerate key security operations functions: detection, investigation, and remediation. People, processes, and technology must all complement one another to create an effective defense from cyberattacks.

Take our free Introduction to Cybersecurity course

People

Users must understand and comply with basic data protection and privacy security principles like choosing strong passwords, being wary of attachments in email, and backing up data. Learn more about basic cybersecurity principles from these Top 10 Cyber Tips (PDF).

Processes

Organizations must have a framework for how they deal with both attempted and successful cyberattacks. One well-respected model, the NIST cybersecurity framework, can guide you. It explains how you can identify attacks, protect systems, detect and respond to threats, and recover from successful attacks.

Technology

Technology is essential to giving organizations and individuals the computer security tools needed to protect themselves from cyberattacks. Three main entities must be protected: endpoint devices like computers, smart devices, and routers; networks; and the cloud. Common technology used to protect these entities include next-generation firewalls, Domain Name System (DNS) filtering, malware protection, antivirus software, and email security solutions.

Why is cybersecurity important?

In today's connected world, everyone benefits from advanced cybersecurity solutions. At an individual level, a cybersecurity attack can result in everything from identity theft to extortion attempts, to the loss of important data like family photos. Everyone relies on critical infrastructure like power plants, hospitals, and financial service companies. Securing these and other organizations is essential to keeping our society functioning.

Everyone also benefits from the work of cyberthreat researchers, like the team of 250 threat researchers at Talos, who investigate new and emerging threats and cyberattack strategies. They reveal new vulnerabilities, educate the public on the importance of cybersecurity, and strengthen open-source tools. Their work makes the internet safer for everyone.

Types of cybersecurity threats

Cloud security

Cloud security provides rapid threat detection and remediation, enhancing visibility and intelligence to prevent malware impacts. It delivers robust protection in multicloud environments, streamlining security without affecting user productivity, and is essential for the safety of applications, data, and users in both hybrid and remote work settings. The scalable nature of cloud security allows for the defense of an expanding array of users, devices, and cloud applications, ensuring comprehensive coverage across all points of potential attack.
Cisco Cloud Protection Suite | Cisco Multicloud Defense

Identity

Identity security and access management involve safeguarding the digital identities of individuals, devices, and organizations. This involves implementing security processes, tools, and policies that control user access to accounts and enable productivity with frictionless access to important information without risk.
The three main goals of identity security are to:

1. Authenticate a user's identity
2. Authorize access to appropriate resources
3. Monitor access activity for weak posture and suspicious activity

Malware

Malware is a type of software designed to gain unauthorized access or to cause damage to a computer.

Phishing

Phishing is the practice of sending fraudulent emails that resemble emails from reputable sources. The aim is to steal sensitive data, such as credit card numbers and login information, and is the most common type of cyberattack. You can help protect yourself through education or a technology solution that filters malicious emails.

Ransomware

Ransomware is a type of malicious software that is designed to extort money by blocking access to files or the computer system until the ransom is paid. Paying the ransom does not guarantee that the files will be recovered or the system restored.

Social engineering

Social engineering is a tactic that adversaries use to trick you into revealing sensitive information. Attackers can solicit a monetary payment or gain access to your confidential data. Social engineering can be combined with any of the threats mentioned above to make you more likely to click on links, download malware, or trust a malicious source.

Threat detection

An effective extended detection and response (XDR) system integrates solutions across the security stack, making it easier for analysts to focus on comprehensive threat detection, prioritize incident response, and improve productivity. With more visibility and context into data security threats, events that would not have been addressed before will surface to a higher level of awareness, thus allowing cybersecurity teams to quickly eliminate any further impact and reduce the severity and scope of the attack.

Read more about XDR | Cisco XDR

Zero trust

Zero trust isn't a single product or technology. It's a security strategy that is best implemented by keeping an organization's business operations, risks, and security outcomes in mind. Although there are various paths to achieving zero trust maturity, most organizations prioritize deployment of technologies such as multi-factor authentication (MFA), device posture checks, zero trust network access (ZTNA), and network segmentation as they implement zero-trust security.
Read more about zero-trust networking | Cisco Duo | Cisco Secure Access

Best practices for cybersecurity

Adopting best practices for cybersecurity can significantly reduce the risk of cyberattacks.

Here are three key practices:

1. Regular software and operating system updates
   Updating software and operating systems regularly helps to patch vulnerabilities and enhance security measures against potential threats.
2. Using strong and unique passwords
   Creating strong and unique passwords for each online account can enhance cybersecurity, as cyberattacks often exploit weak or stolen passwords.
3. Implementing multi-factor authentication (MFA)
   Multi-factor authentication involves multiple identification forms before account access, reducing the risk of unauthorized access. Cisco Duo includes MFA that can integrate with most major applications as well as custom apps.

Following these practices enhances cybersecurity and protects digital assets. It's vital to stay vigilant and informed about the latest threats and security measures to stay ahead of cybercriminals.

What is the difference between cybersecurity and information security?

Information security (InfoSec) protects all forms of information, digital and physical. Cybersecurity protects all forms of digital information, including computers, handheld devices, cloud, and networks, and can be considered a subset of InfoSec.

Types of InfoSec

Application security

Application security is a broad topic that covers software vulnerabilities in web and mobile applications and application programming interfaces (APIs). These vulnerabilities may be found in authentication or authorization of users, integrity of code and configurations, and mature policies and procedures. Application vulnerabilities can create entry points for significant InfoSec breaches. Application security is an important part of perimeter defense for InfoSec.

Cloud security

Cloud security focuses on building and hosting secure applications in cloud environments and securely consuming third-party cloud applications. “Cloud” simply means that the application is running in a shared environment. Businesses must make sure that there is adequate isolation between different processes in shared environments.

Cryptography

Encrypting data in transit and data at rest helps ensure data confidentiality and integrity. Digital signatures are commonly used in cryptography to validate the authenticity of data. Cryptography and encryption has become increasingly important. A good example of cryptography use is the Advanced Encryption Standard (AES). The AES is a symmetric key algorithm used to protect classified government information.

Infrastructure security

Infrastructure security deals with the protection of internal and extranet networks, labs, data centers, servers, desktops, and mobile devices.

Incident response

Incident response is the function that monitors for and investigates potentially malicious behavior.

In preparation for breaches, IT staff should have an incident response plan for containing the threat and restoring the network. In addition, the plan should create a system to preserve evidence for forensic analysis and potential prosecution. This data can help prevent further breaches and help staff discover the attacker.

Vulnerability management

Vulnerability management is the process of scanning an environment for weak points (such as unpatched software) and prioritizing remediation based on risk.

In many networks, businesses are constantly adding applications, users, infrastructure, and so on. For this reason, it is important to constantly scan the network for potential vulnerabilities. Finding a vulnerability in advance can save your businesses the catastrophic costs of a breach.

A primer on firewalls

A firewall is a network security device that separates a trusted internal network from an external network deemed untrustworthy, such as the internet. It regulates incoming and outgoing network traffic based on preset security rules. Firewalls are paramount in shielding networks from unauthorized access, harmful activities, and potential threats, and can exist as hardware, software, software-as-a-service (SaaS), or public or private (virtual) cloud.
Firewalls scrutinize network packets and implement security policies, effectively barring unauthorized users or potentially harmful data from infiltrating or exiting a network. Notably, firewalls serve as gatekeepers, scrutinizing each network packet and deciding whether to permit or block it based on pre-set rules. This helps to ensure that only traffic deemed safe and legitimate is allowed through the firewall.

In addition to these core functions, today's next-generation firewalls (NGFWs) have a range of features to bolster network security. These include deep packet inspection, application visibility and control, intrusion detection and prevention, malware defense, URL filtering, and more.

Types of firewalls

Packet filtering firewall

These firewalls scrutinize each packet of data that passes through them, and then filters them based on parameters like source and destination IP addresses, port numbers, and protocol types. While these firewalls are relatively simple and cost-effective, they are unable to examine the contents of packets, which makes them less effective against sophisticated attacks.

Proxy firewall

A proxy firewall is an early type of firewall device, serving as the gateway from one network to another for a specific application. Proxy servers can provide additional functionality, such as content caching and security, by preventing direct connections from outside the network. However, this also may impact throughput capabilities and the applications they can support.

Stateful inspection firewall

Now considered a traditional firewall, a stateful inspection firewall allows or blocks traffic based on state, port, and protocol. It monitors all activity from the opening of a connection until it is closed. Filtering decisions are made based on both administrator-defined rules as well as context, which refers to using information from previous connections and packets belonging to the same connection.

Web application firewall (WAF)

Web application firewalls act as intermediaries for internal and external networks, handling all communication requests on behalf of the internal network. They offer a high level of security, as they can inspect the content of packets and filter out malicious or unauthorized data. However, their reliance on proxy servers can introduce latency and impact network performance.

Unified threat management (UTM) firewall

A UTM device typically combines, in a loosely coupled way, the functions of a stateful inspection firewall with intrusion prevention and antivirus. It may also include additional services and often cloud management. UTMs focus on simplicity and ease of use.

Explore UTM devices

Next-generation firewall (NGFW)

A next-generation firewall (NGFW) is a network security device that provides capabilities beyond a traditional, stateful firewall. While a traditional firewall typically provides stateful inspection of incoming and outgoing network traffic, a next-generation firewall includes additional features like application awareness and control, intrusion prevention system (IPS),

URL filtering based on geolocation and reputation, and threat intelligence. An NGFW can ease administration and reduce complexity with unified policies that protect across the entire attack continuum.

Explore next-generation firewalls

AI-powered firewall

AI-powered firewalls use artificial intelligence (AI) and machine learning (ML) to enhance threat protection and network security. While traditional firewalls use predetermined rules to block and detect threats, AI-powered firewalls work in real time to analyze dynamic network traffic, identify patterns, and help organizations automate lifecycle management of their firewall policy.

Virtual firewall

A virtual firewall is typically deployed as a virtual appliance. It can be hosted on-premises in a private cloud environment based on VMware ESXi, Microsoft Hyper-V, KVM, OpenStack, and Nutanix. A virtual firewall can also be deployed in a public cloud infrastructure, such as Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), Oracle Cloud Infrastructure (OCI). With a virtual firewall, you can secure your applications and data across the multicloud environments with unified policy controls, centralized management, and advanced threat defense.

Explore virtual firewalls for public cloud and private cloud

Cloud-native firewall

Cloud-native firewalls modernize the way to secure applications and workload infrastructure at scale. With automated scaling features, cloud-native firewalls enable networking operations and security operations teams to run at agile speeds. A cloud-native firewall supports agile and elastic security, multi-tenant capability, and smart load balancing.

What is the intent of malware?

Malware is developed as harmful software that invades or corrupts your computer network. The goal of malware is to cause havoc and steal information or resources for monetary gain or sheer sabotage intent.

Intelligence and intrusion

Exfiltrates data such as emails, plans, and especially sensitive information like passwords.

Disruption and extortion

Locks up networks and PCs, making them unusable. If it holds your computer hostage for financial gain, it's called ransomware.

Destruction or vandalism

Destroys computer systems to damage your network infrastructure.

Steal computer resources

Uses your computing power to run botnets, cryptomining programs (cryptojacking), or send spam emails.

Monetary gain

Sells your organization's intellectual property on the dark web.

How do I protect my network against malware?

Typically, businesses focus on preventative tools to stop breaches. By securing the perimeter, businesses assume they are safe. However, some advanced malware will eventually make their way into your network. As a result, it is crucial to deploy technologies that continually monitor and detect malware that has evaded perimeter defenses. Sufficient advanced malware protection requires multiple layers of safeguards along with high-level network visibility and intelligence.

types of malware

Virus

Viruses are a subgroup of malware. A virus is malicious software attached to a document or file that supports macros to execute its code and spread from host to host. Once downloaded, the virus will lie dormant until the file is opened and in use. Viruses are designed to disrupt a system's ability to operate. As a result, viruses can cause significant operational issues and data loss.

Worms

A worm is a type of malicious software that rapidly replicates and spreads to any device within the network. Unlike viruses, worms do not need host programs to disseminate. A worm infects a device through a downloaded file or a network connection before it multiplies and disperses at an exponential rate. Like viruses, worms can severely disrupt the operations of a device and cause data loss.

Trojan virus

Trojan viruses are disguised as helpful software programs. But once the user downloads it, the Trojan virus can gain access to sensitive data and then modify, block, or delete the data. This can be extremely harmful to the performance of the device. Unlike normal viruses and worms, Trojan viruses are not designed to self-replicate.

Spyware

Spyware is malicious software that runs secretly on a computer and reports back to a remote user. Rather than simply disrupting a device's operations, spyware targets sensitive information and can grant remote access to predators. Spyware is often used to steal financial or personal information. A specific type of spyware is a keylogger, which records your keystrokes to reveal passwords and personal information.

Adware

Adware is malicious software used to collect data on your computer usage and provide appropriate advertisements to you. While adware is not always dangerous, in some cases adware can cause issues for your system. Adware can redirect your browser to unsafe sites, and it can even contain Trojan horses and spyware. Additionally, significant levels of adware can slow down your system noticeably. Because not all adware is malicious, it is important to have protection that constantly and intelligently scans these programs.

Ransomware

Ransomware is malicious software that gains access to sensitive information within a system, encrypts that information so that the user cannot access it, and then demands a financial payout for the data to be released. Ransomware is commonly part of a phishing scam. By clicking a disguised link, the user downloads the ransomware. The attacker proceeds to encrypt specific information that can only be opened by a mathematical key they know. When the attacker receives payment, the data is unlocked.

Fileless malware

Fileless malware is a type of memory-resident malware. As the term suggests, it is malware that operates from a victim's computer's memory, not from files on the hard drive. Because there are no files to scan, it is harder to detect than traditional malware. It also makes forensics more difficult because the malware disappears when the victim computer is rebooted. In late 2017, the Cisco Talos threat intelligence team posted an example of fileless malware that they called DNSMessenger.

What are the benefits of advanced malware protection?

Advanced malware can take the form of common malware that has been modified to increase its capability to infect. It can also test for conditions of a sandbox meant to block malicious files and attempt to fool security software into signaling that it is not malware. Advanced malware protection software is designed to prevent, detect, and help remove threats in an efficient manner from computer system.

What is social engineering?

Social engineering attacks manipulate people into sharing information that they shouldn't share, downloading software that they shouldn't download, visiting websites they shouldn't visit, sending money to criminals or making other mistakes that compromise their personal or organizational security.

An email that seems to be from a trusted coworker requesting sensitive information, a threatening voicemail claiming to be from the IRS and an offer of riches from a foreign potentate are just a few examples of social engineering. Because social engineering uses psychological manipulation and exploits human error or weakness rather than technical or digital system vulnerabilities, it is sometimes called "human hacking."

Cybercriminals frequently use social engineering tactics to obtain personal data or financial information, including login credentials, credit card numbers, bank account numbers and Social Security numbers. They use the information that they have stolen for identity theft, enabling them to make purchases using other peoples' money or credit, apply for loans in someone else's name, apply for other peoples' unemployment benefits and more. But a social engineering attack can also be the first stage of a larger-scale cyberattack. For example, a cybercriminal might trick a victim into sharing a username and password and then use those credentials to plant ransomware on the victim's employer's network.

Social engineering is attractive to cybercriminals because it enables them to access digital networks, devices and accounts without having to do the difficult technical work of getting around firewalls, antivirus software and other cybersecurity controls. This is one reason why social engineering is the leading cause of network compromise today according to ISACA's State of Cybersecurity 2022 report. According to IBM's *Cost of a Data Breach* report, breaches caused by social engineering tactics (such as phishing and business email compromise) were among the most costly.

How and why social engineering works

Social engineering tactics and techniques are grounded in the science of human motivation. They manipulate victims' emotions and instincts in ways proven to drive people to take actions that are not in their best interests.

Most social engineering attacks employ one or more of the following tactics:

- **Posing as a trusted brand**: Scammers often impersonate or "spoof" companies that victims know, trust and perhaps do business with often or regularly—so regularly that they follow instructions from these brands reflexively, without taking the proper precautions. Some social engineering scammers use widely available kits for staging fake websites that resemble those of major brands or companies.
- **Posing as a government agency or authority figure**: People trust, respect or fear authority (in varying degrees). Social engineering attacks play on these instincts with messages that appear or claim to be from government agencies (example: the FBI or IRS), political figures or even celebrities.
- **Inducing fear or a sense of urgency**: People tend to act rashly when scared or hurried. Social engineering scams can use any number of techniques to induce fear or urgency in victims. For instance, telling the victim that a recent credit transaction was not approved, that a virus has infected their computer, that an image used on their website violates a copyright and so on. Social engineering can also appeal to victims' fear of missing out (FOMO), which creates a different kind of urgency.
- **Appealing to greed**: The Nigerian Prince scam, an email wherein someone claiming to be a Nigerian royal trying to flee his country offers a giant financial reward in exchange

for the recipient's bank account information or a small advance fee, is one of the best-known examples of social engineering that appeals to greed. This type of social engineering attack can also come from an alleged authority figure and creates a sense of urgency, which is a powerful combination. This scam is as old as email itself, but was still raking in USD 700,000 per year as of 2018.

- **Appealing to helpfulness or curiosity**: Social engineering ploys can also appeal to victims' better nature. For instance, a message that appears to be from a friend or a social networking site can offer technical help, ask for participation in a survey, claim that the recipients' post has gone viral and provide a spoofed link to a fake website or malware download.

Types of social engineering attacks

Phishing

Phishing attacks are digital or voice messages that try to manipulate recipients into sharing sensitive information, downloading malicious software, transferring money or assets to the wrong people or taking some other damaging actions. Scammers craft phishing messages to look or sound like they come from a trusted or credible organization or individual—sometimes, even an individual the recipient knows personally.

There are many types of phishing scams:

- **Bulk phishing emails** are sent to millions of recipients at a time. They appear to be sent by a large, well-known business or organization, such as a national or global bank, a large online retailer, a popular online payments provider and so on, and make a generic request such as "*we're having trouble processing your purchase, please update your credit information*." Frequently, these messages include a malicious link that takes the recipient to a fake website that captures the recipient's username, password, credit card data and more.
- Spear phishing targets a specific individual, typically one with privileged access to user information, the computer network or corporate funds. A scammer will research the target, often using information that is found on LinkedIn, Facebook or other social media to create a message that appears to come from someone the target knows and trusts or

that refers to situations with which the target is familiar. Whale phishing is a spear phishing attack that targets a high-profile individual, such as a CEO or political figure. In business email compromise (BEC), the hacker uses compromised credentials to send email messages from an authority figure's actual email account, making the scam that much more difficult to detect.

- **Voice phishing or vishing**, is phishing that is conducted through phone calls. Individuals typically experience vishing in the form of threatening recorded calls claiming to be from the FBI.
- SMS phishing, or smishing, is phishing through a text message.
- **Search engine phishing** involves hackers creating malicious websites that rank high in search results for popular search terms.
- **Angler phishing** is phishing using fake social media accounts that masquerade as the official accounts of trusted companies' customer service or customer support teams.

According to the *IBM X-Force® Threat Intelligence Index*, phishing is the leading malware infection vector, identified in 41% of all incidents. According to the *Cost of a Data Breach* report, phishing is the initial attack vector leading to the most costly data breaches.

Baiting

Baiting lures (no pun intended) victims into knowingly or unwittingly giving up sensitive information or downloading malicious code by tempting them with a valuable offer or even a valuable object.

The Nigerian Prince scam is probably the best-known example of this social engineering technique. More current examples include free but malware-infected games, music or software downloads. But some forms of baiting are barely artful. For example, some threat actors leave malware-infected USB drives where people will find them, grab them and use them because "hey, free USB drive."

Tailgating

In tailgating, also called "piggybacking", an unauthorized person closely follows an authorized person into an area containing sensitive information or valuable assets. Tailgating can be conducted in person, for example, a threat actor can follow an employee through an unlocked door. But tailgating can also be a digital tactic, such as when a person leaves a computer unattended while still logged in to a private account or network.

Pretexting

In pretexting, the threat actor creates a fake situation for the victim, and poses as the right person to resolve it. Very often (and most ironically) the scammer claims that the victim has been

impacted by a security breach, and then offers to fix things if the victim will provide important account information or control over the victim's computer or device. Technically speaking, almost every social engineering attack involves some degree of pretexting.

Quid pro quo

In a quid pro quo scam, hackers dangle a desirable good or service in exchange for the victim's sensitive information. Fake contest winnings or seemingly innocent loyalty rewards ("thank your for your payment, we have a gift for you") are examples of quid pro quo ploys.

Scareware

Also considered a form of malware, scareware is software that uses fear to manipulate people into sharing confidential information or downloading malware. Scareware often takes the form of a fake law enforcement notice accusing the user of a crime, or a fake tech support message warning the user of malware on their device.

Watering hole attack

From the phrase "somebody poisoned the watering hole", hackers inject malicious code into a legitimate web page that is frequented by their targets. Watering hole attacks are responsible for everything, from stolen credentials to unwitting drive-by ransomware downloads.

Social engineering defenses

Social engineering attacks are notoriously difficult to prevent because they rely on human psychology rather than technological pathways. The attack surface is also significant: In a larger organization, it takes just one employee's mistake to compromise the integrity of the entire enterprise network. Some of the steps that experts recommend to mitigate the risk and success of social engineering scams include:

- **Security awareness training**: Many users don't know how to identify social engineering attacks. In a time when users frequently trade personal information for goods and services, they don't realize that surrendering seemingly mundane information, such as a phone number or date of birth, can allow hackers to breach an account. Security awareness training, combined with data security policies, can help employees understand how to protect their sensitive data and how to detect and respond to social engineering attacks in progress.
- **Access control policies**: Secure access control policies and technologies, including multi-factor authentication, adaptive authentication and a zero trust security approach can limit cybercriminals' access to sensitive information and assets on the corporate network even if they obtain users' login credentials.

- **Cybersecurity technologies**: Spam filters and secure email gateways can prevent some phishing attacks from reaching employees in the first place. Firewalls and antivirus software can mitigate the extent of any damage done by attackers who gain access to the network. Keeping operating systems updated with the latest patches can also close some vulnerabilities that attackers exploit through social engineering. Additionally, advanced detection and response solutions, including endpoint detection and response (EDR) and extended detection and response (XDR), can help security teams quickly detect and neutralize security threats that infect the network through social engineering tactics.

Sources : Cisco site and IBM and Questions of my mind and Some Definitions of some Famous & important topics

Prepared by : Yusuf Yasser said

ID: 22100809