Cybersecurity: Fundamentals to Consider

Independent Learner's Guide

Copyright

Disclaimer

We make a sincere effort to ensure the accuracy of the material described herein; however there is no warranty, expressed or implied, with respect to the quality, correctness, reliability, accuracy, or freedom from error of this document or the products it describes. Information used in examples are intended to be fictional. Any resemblance to real persons or companies is entirely coincidental.

Table of Contents

OVERVIEW

Cybersecurity is the protection of Internet-connected systems such as hardware, software and data from cyber-threats. The practice is used by individuals and enterprises to protect against unauthorized access to data centers and other computerized systems.

Cyberattacks are increasing at an alarming rate. It was estimated that in 2018 there were 2.3 billion data breaches – almost three times more than the year before – which cost business over $600 billion. It has only got worse since that year.

While most businesses have installed forms of cybersecurity (i.e. firewalls and other defenses to stop attacks), these are not foolproof. One of the key risk factors in cyberattacks is human error. A recent Intel Security survey found that 97 per cent of people could not identify all the phishing emails in a sample of 10 emails.

The need for all employees to be aware of and active in protecting their workplace data is the foundation of effective security.

Objectives

At the end of this workshop, you will be able to:

- Understand the history and the current state of cyberattacks in terms of quantity and cost to business.
- Name and explain the methods used in various types of cyberattacks.
- Outline the risk of human error in inadvertently contributing to the success of cyberattacks.
- Have an appreciation of company-wide measures to protect against cyberattacks and their role in the success of these defense measures.
- Explain the importance of a company culture that focuses on cybersecurity to successfully defend against attacks.
- Realize the social media mining activities of cyber criminals and be better able to practice safe social media behavior.
- Outline the information needed in a social media security policy.
- Understand and practice good security behaviors when working remotely or travelling.
- Recognize phishing attacks by identifying the subtle clues that are present in all phishing attacks.
- When a cyberattack has been successful, understand what steps to take to mitigate the effect.

THE STATE OF CYBERCRIME

To start our exploration of cybersecurity, it is important to understand the impact that cyberattacks can have on business. Let's look at the history of cybercrime and its associated costs.

History of Cybercrime

"The modern thief can steal more with a computer than a gun." – National Research Council, "Computers at Risk," 1991.

Cybercrime is defined as an illegal or unethical activity committed using the internet or a computer. The activity can be against people, property or governments.

Cybercrime has been around since the invention of the computer.

Historical Examples of Cybercrime

Robert Herjavec, in an essay entitled *Cybersecurity CEO: The History of Cybercrime, From 1834 To Present*, outlines some of the most interesting **historical** examples of cybercrime. Some of the early examples include:

- **1834** – French Telegraph System — A pair of thieves hack the French Telegraph System and steal financial market information, effectively conducting the world's first cyberattack.
- **1878** – Two years after Alexander Graham Bell invents the telephone, the Bell Telephone Company removes a group of teenage boys from the telephone system in New York for repeatedly and intentionally misdirecting and disconnecting customer calls.
- **1940** – Rene Carmille, a member of the Resistance in Nazi-occupied France and a punch-card computer expert who owns the machines that the Vichy government of France uses to process information, finds out that the Nazis are using punch-card machines to process and track down Jews, volunteers to let them use his system, and then hacks them to thwart their plan.
- **1969** – An anonymous person installs a program (RABBITS Virus) on a computer at the University of Washington Computer Center. The inconspicuous program makes copies of itself (breeding like a rabbit) until the computer overloads and stops working. This is thought to be the very first computer virus.

- **1970-1995** – Beginning in 1970, Kevin Mitnick penetrates some of the most highly-guarded networks in the world, including Nokia and Motorola, using elaborate social engineering schemes, tricking insiders into handing over codes and passwords, and using the codes to access internal computer systems. He becomes the most-wanted cybercriminal of the time.
- **1981** – Ian Murphy, also known as "Captain Zap," hacks into the AT&T network and changes the internal clock to charge off-hour rates at peak times. The first person convicted of a cybercrime, he is sentenced to 1,000 hours of community service and two-and-a-half years of probation.
- **1982** – The CIA blows up a Siberian Gas pipeline without the use of a bomb or a missile by inserting a code into the network and the computer system in control of the gas pipeline. The code was embedded into equipment purchased by the Soviet Union from a company in Canada.
- **1988** – Robert Morris creates what would be known as the first worm on the internet. The worm is released from a computer at MIT to suggest that the creator is a student there. The potentially harmless exercise quickly became a vicious denial of service attack when a bug in the worm's spreading mechanism leads to computers being infected and reinfected at a rate much faster than he anticipated.
- **1989** – A diskette claiming to be a database of AIDS information is mailed to thousands of AIDS researchers and subscribers to a UK computer magazine. It contains a Trojan (after the Trojan Horse of Greek mythology), or destructive program masquerading as a benign application.
- **1999** – Jonathan James, 15, manages to penetrate U.S. Department of Defense division computers and install a backdoor on its servers, allowing him to intercept thousands of internal emails from different government organizations, including ones containing usernames and passwords for various military computers. Using the info, he steals a piece of NASA software. Systems are shut down for three weeks.
- **2000** –Michael Calce (also known as MafiaBoy) a 15-year-old Canadian high school student, unleashes a DDoS attack on several high-profile commercial websites including Amazon, CNN, eBay and Yahoo. An industry expert estimates the attacks resulted in $1.2 billion dollars in damages.

In a 2019 Cybersecurity research report, a survey of 267 cybersecurity experts and Information Systems Security Association organizations revealed that 91 per cent of organizations believe they are at risk for a significant cyberattack. Significantly, when asked about the root cause of the risk, 34 per cent identified lack of end-user training even though they also reported 46 per cent of companies over the previous two years had increased the amount of training for non-technical employees.

Cost of Cybercrime

Herjavec also outlines the magnitude of more recent cybercrimes. Here are some examples that have occurred since 2015:

- Health insurer Anthem reports theft of personal information from as many as 78.8 million current and former customers.
- LockerPin ransomware resets the pin code on Android phones and demands $500 from victims to unlock the device.
- A worldwide gang of criminals steals a total of $45 million in a matter of hours by hacking a database of prepaid debit cards and then draining cash machines around the globe.
- United States Democratic National Committee emails are leaked to and published by WikiLeaks prior to the 2016 U.S. presidential election.
- Equifax, one of the largest U.S. credit bureaus, is hacked, exposing 143 million user accounts. The sensitive leaked data includes Social Security numbers, birth dates, addresses, driver's license numbers, and some credit card numbers.
- An Eastern European criminal gang that is targeting restaurants uses phishing to steal credit card information of millions of Chipotle restaurant customers.
- WannaCry, the first known example of ransomware operating via a worm (viral software that replicates and distributes itself), targets a vulnerability in older versions of Windows OS. Within days, tens of thousands of businesses and organizations across 150 countries are locked out of their own systems by WannaCry's encryption. The attackers demand $300 per computer to unlock the code.
- 74 Facebook groups devoted to the sale of stolen credit card data, identity info, spam lists, hacking tools, and other cybercrime commodities are uncovered.

The Nineth Annual Cost of Cybercrime Study looked at cybercrime activity in 11 countries and identified an 11 per cent increase in security breaches from 2017 to 2018. More than 30 per cent of attacks were through malware and web-based attacks, although the largest increase in cyberattacks came from malicious insiders. The cost of these breaches was $13 million for each company up from $11.7 million the year before. This does not include cyberattacks stopped by firewalls and other defense technologies.

Radware reported that there were 2.3 billion data breaches in 2018, almost three times more than the year before, costing companies about $600 billion.

The losses from cybercrime are not just monetary. According to Radware, there are three major impacts from a cyberattack that a company needs to consider:

- Customer loss can be as large as 41 per cent.
- Reputation loss can be as high as 34 per cent.
- Operational loss can be as high as 34 per cent.

A 2018 Gartner report, The Urgency to Treat Cybersecurity as a Business Decision, forecasted that in 2019, companies would spend $124 billion US on defense technologies.

TYPES OF CYBERATTACKS

There have been a huge number of cyberattacks and the costs involved for organizations targeted by these attacks is immense. It is important to understand the wide variety of methods used in cyberattacks.

You will now look at the various ways your business or organisation can be victimized.

Types of Attacks

In the space below, brainstorm the various types of cybercrimes that you have heard of:

Types of Cybersecurity Threats

The process of keeping up with new technologies, security trends and threat intelligence is a challenging task. However, it is necessary in order to protect information and other assets from cyber threats, which take many forms. Cyber threats can include:

Malware is a form of malicious software, which any file or program can be used to harm a computer user, such as worms, computer viruses, Trojan horses and spyware.

Ransomware attacks are a type of malware that involves an attacker locking the victim's computer system files -- typically through encryption -- and demanding a payment to decrypt and unlock them.

Social engineering is an attack that relies on human interaction to trick users into breaking security procedures to gain sensitive information that is typically protected.

Phishing is a form of fraud where fraudulent emails are sent that resemble emails from reputable sources; however, the intention of these emails is to steal sensitive data, such as credit card or login information.

ROLE OF HUMAN ERROR

Let’s look at how employees contribute to the success of cyberattacks.

The Role of Human Error

Many companies have installed firewalls to stop cyberattacks, but they are not foolproof. They do not protect against email-based threats or unauthorized access to devices. As well, criminals are always trying to breach firewalls to continue to have access to communications through unsuspecting employees. Firewalls are a layer of protection, but other layers are needed.

In fact, for many companies, human error is their biggest risk. If employees cannot recognize a threat, they will not know what to do and may inadvertently give criminals what they are looking for. That is why a critical layer of defense is well-trained employees.

But how successful are phishing attacks, especially those from emails?

The 2020 State of the Phishing Report found that 55 per cent of companies surveyed have dealt with at least one successful phishing attack in 2019.

Intel Security surveyed 19,000 respondents in 144 countries and found that 97 per cent of people could not identify all the phishing emails in a sample of 10 emails.

A Statista report found that spam messages accounted for almost 54 per cent of email traffic in March 2020.

While not all these emails are malicious, it still means that human training is very important.

Opening Email

In a recent blog, Patrick Nohe listed some of the most-clicked email subject lines.

Rank the subject lines from most likely to be clicked on to least likely. Also, estimate the percentage of people who clicked on each email.

Rank	Subject Lines	%
	Please Read Important Message from Human Resources	
	Official Data Breach Notification	
	Change of Password Required Immediately	
	Revised Vacation & Sick Time Policy	
	IT Reminder: Your Password Expires in Less Than 24 Hours	
	UPS Label Delivery 1ZBE312TNY00015011	

WHAT CAN A BUSINESS DO?

Let's look at defenses that organizations can mount to protect themselves, as well as why employees need to be careful about what they post on social media.

Business-Wide Defenses

Many employees may not realize some of the behind-the-scenes defenses that are already in place at their company. Below are some additional protections that could be used:

- Use of an exchange server rather than a public cloud platform for sensitive data (high risk or high-profile emails, accounts and communications)
- Use of an SSL Certificate that secures transactions by providing a third-party authentication
- Strict approval processes for accounting that includes two-step verification (email plus phone, text or in person) or requires approval by the manager and accounting personnel. This verification could be set up for money transfers above a certain value.
- Strict approval processes for human resources that includes multiple 'sign offs' on release of sensitive information.

- Use of a secure gateway Hosted Payment service. The provider assures that all processes are up-to-date, and payments are encrypted.
- Use of single sign-on (SSO) that uses a single login and password for all systems with strong third-party authentication tokens.
- Conduct regular penetration testing to see if there are vulnerabilities to cyberattacks within the company.
- Encourage healthy skepticism. If it looks like it might be a cyberattack treat it as a cyberattack.
- Review any company information that is made public (newsletters, annual reports, blogs, tweets, etc.) to see if it could be used by a cyber attacker.

A company's culture is an important component of susceptibility to cyberattacks. Cyberattacks are less successful in companies that have a collaborative culture. In these companies, employees will ask for help and check with co-workers. A progressive hierarchy culture where employee actions are not governed by strict authoritarian rule is also good for minimizing attacks.

It is important for employees to feel comfortable talking to their supervisor or contacting the IT Department when they suspect a **cyberattack**. *The fear of clicking **on a suspicious email** should be **greater** than the fear of the IT Department.*

Focus on Social Media

Social media is an area where cyber attackers mine information about companies and individuals.

Cyber attackers can easily learn about a company's senior leaders, responsibilities, awards, etc. from a company's website. Add in company and personal social media and it is possible to discern likes, hobbies, activities, favorite restaurants and even when employees are on vacation. All of this information can be used by a cyber attacker to make their scheme look more real.

How it Can Work

You just posted a picture of you standing on the dock in front of your cottage holding that five-pound trout you caught during your month-long vacation in July. You just gave a criminal everything they know to come out and steal all your valuables at the cottage. The criminal can use the location tag on your picture to proceed to the cottage. Chances are you are not going to be there for another long vacation. In the background they saw a Tiffany lamp in the window, a satellite dish (probably hooked up to a big screen TV) and just off to the right, a shed with an open door revealing a new chainsaw, fishing gear and a set of golf clubs. The rest of what is in the house he can envisage on his own. Great target.

It is easy for a criminal, cyber or otherwise, to glean information from your social media. But most cybercriminals are not interested in those physical items. They are interested in the information you gave them, especially if they can tie it to your workplace. That comes when

someone from the office likes your photo and says they cannot wait for you to get back to work. The cyber criminal then checks their profile that tells them where you work. From there the criminal can check out the contact page on your company website and get your email. Now the scammer can email you a fake offer for a round of golf, fishing trip or upgrade to your satellite dish with a malicious link, and you might just fall for it.

How do you make sure this does not happen?

The first step is to develop a social media security policy.

Create a Social Media Policy

Brainstorm what information you think should be included in a social media security policy. Write your ideas in the space below.

BEST PRACTICES FOR REMOTE OR TRAVELLING EMPLOYEES

No business is totally protected from cyberattacks, but if employees are working from home or travelling, there are new vulnerabilities that need to be addressed.

Let's look at how out-of-office workers can make sure they do not expose their organization to threats.

Out of Office Protections

Consider the following scenario.

Imagine that you are no longer within the relatively safe confines of the office. You are travelling to visit a number of clients throughout the country over the next two weeks.

What company procedures and personal behaviors need to be in place to minimize a potential security breach?

CYBERATTACKS ON INDIVIDUALS

In this session, we explore various techniques that cybercriminals use to target employees, including spam, phishing, social engineering, malware, and social media.

Cyberattacks to Obtain Sensitive Information

Phishing attacks are always evolving and get more and more creative. Here are the main forms of phishing attacks.

Spam

Spam is an unsolicited email message sent out to numerous recipients at the same time. Much of the spam is someone trying to sell you a product or service and is not malicious – it is just junk.

Increasingly malicious spam is making its way to social media as invitations to connect, fake job opportunities, and other similar schemes. Cyber criminals use the trust you have built up with the social media site to lure you into responding. In doing so they can unleash embedded malware to steal information from your social media activity.

Phishing

Phishing is a popular method of attack. Phishing attacks are often emails that are sent to thousands of random individuals. The attacker poses as a legitimate person or institution to gain your trust. These communications look deceptively real and often include logos, font types, etc. that look just like the real thing.

The bait may come as a request to follow a link (to accept your lottery win or a preapproved line of credit, etc.). They may also invite you to connect on a social media site (e.g. LinkedIn).

Once you click on the link it can send you to a deceptively real-looking website that asks for sensitive information such as username, email address, and passwords that they can use to access your social media accounts and bank login. It may also unleash malware that infects your computer and extracts personal information.

Social Engineering

Social engineering phishing attacks rely on social psychology and manipulation to get people to perform an action that can make information available to the criminal perpetrator. The information could include information about the person's identification, computer passwords, financial access, etc. They can be unleashed through email, web, phone, USB drives, or other mediums.

Using this false trust, the attacker can gain access to a great number of resources. In a corporate environment a criminal can create an email that seemingly comes from tech support to fool you into thinking that you need to click on a link to update software or change

your password. Once you click, they can download malware, hijack your password or any number of important pieces of information.

Here are some variations of phishing cyberattacks:

Spear phishing	Spear phishing is more targeted than phishing. The attack could be on a single high-profile individual or organization. Using widely available information (from social media, blog sites, personal and corporate websites) and illegally gained information (security leaks, hacking, etc.) they create emails that look and feel like real ones from a trusted friend or colleague. Once gaining the full trust of the target, the attackers can then steal information, and/or install malware.
Whaling	Whaling is spear phishing when the target individual is a senior executive.
Vishing	Not all phishing uses emails or the internet. Vishing can come on the phone from someone pretending to be from a legitimate company. Most people are familiar with the "Hello, you have won a free cruise" calls that offer a free prize but require you to pay for shipping and handling or a redemption fee first or ask you to provide personal information such as a credit card number. When attacking a company, the perpetrator will mimic a company's IVR system message to trick people into calling a fraudulent toll-free number to extract information from them.
Smishing	Smishing works the same as Vishing but comes as a text message.

Other attack methods:

Baiting	Baiting, like many of the techniques that we have talked about, is designed to place malicious software on your computer. Physical baiting is not done over the internet. Instead, someone leaves malicious software on a flash drive in a public area (restaurants, bus stations, churches, etc.) in hopes that someone will pick it up and put it in their computer to see what is on it. Digital baiting hides malicious software in 'free' downloads or fraudulent software updates on the internet.
Tailgating	When a criminal wants to target specific individuals or organizations, they will hack into free Wi-Fi in cafes or restaurants where they know the targets frequent (perhaps a café across from

	the head office) to obtain personal information they can use to hack into computers or offices.
Pretexting	In pretexting, the criminal will impersonate (by phone, email, text message) a police officer, revenue agent or even a co-worker, to collect personal information. Usually, they say they need a critical piece of information that will keep the employee from legal or financial trouble.
Fraudulent Websites	Fraudulent websites are built to try to make you think you are on the real website of a particular company. Then when you provide login details, the scammer can use them to try and access other accounts that you have. You think you are renewing a membership, but you are giving scammers information they can use against you. You can be lured to these sites by increasing numbers of fake ads on Google, Facebook, and other platforms.
False or Fake Advertisements	Scammers realize that there are millions of ads on websites and social media and have begun embedding these ads with malware. You are looking at a legitimate ad, but you get much more than you bargained for when you click on it.

Malware (Malicious Software)

Malware is a package that a cyber criminal wants to place on your computer.

We have mentioned malware a couple times already. It is software that has been developed to damage or steal information from any device to which it is downloaded. The most common malware tools are worms and Trojans, but others include viruses, bots, bugs and spyware.

Malware can be developed to attack specific companies' computer systems to obtain particular information or destroy the network. Variations of malware include:

Worm	Worms are programs that when they reach your system independently self-replicate at will.
Trojan	Trojan viruses look like legitimate software (perhaps fake anti-virus software) but when you have installed them, they can delete, block, modify, or copy data from your computer. They can also disrupt the performance of your computer or network.
Botnet	Botnets are designed to attack control devices in homes – things such as remote controllers, smart speakers, appliances and other Internet of Things devices. These botnets can be used to steal

	information that can be used to attack other personal objects and accounts that use the same credentials.
Viruses	Like biological viruses, they are small pieces of code that attach themselves to legitimate code in your device and attack your system files.
Spyware	Spyware sits on your computer tracking sites you visit, personal information you use for logins, filling out forms, etc.
Ransomware	Ransomware's purpose is to extort money from a target. The ransomware infects a computer or network of computers. The criminals will require the individual or company to pay a ransom (usually in untraceable bitcoins) to stop them from shutting down the computers or to release them. A notice that the computer(s) have been compromised pops up on the screen with instructions of how to pay the ransom.
Scareware	Unlike Ransomware, Scareware is not directed at a target. It is usually a popup when you are browsing the internet. It tells you that it has detected malware or viruses on your computer and prompts you to download a fix to prevent your computer from being compromised or wiped out. When the victim downloads the fix, they are actually downloading malware that gives the criminals access to your computer and information stored there. The warning can look like it comes from a reputable company (Norton, MacAfee, etc.). A variation is a popup that threatens that they will contact the FBI or other police organization. This is usually if you have opened a site that provide free resources for something that is not typically free (e.g. Microsoft Office, Sage, etc.).

Social Media

Remember the post about the five-pound trout that we mentioned earlier, which resulted in a scammer learning all those things about you? Well, most people engaging in illicit activities do not wait for you to inadvertently give them information. Many set up traps for you on social media. Here are some of the ways:

Fake customer service accounts	Many big brands have customer service and support on their social media platforms. But you need to be careful because scammers know this too and they create authentic looking branded sites. You may be on one of their sites giving details about yourself, but you will never get the service or support, only a cyberattack.
Account cancellation scam	In this scam you will receive an email or text announcing that your social media account will be cancelled unless you verify your account information by clicking on the link provided. Of course, it is a bad link. Usually, you are told you must do this in the next 10 minutes (or some quick turnaround time) in hopes that you will not have time to think very much about what you are doing.
Fake lottery or prize winnings	You have seen these popups on websites or posts on social media telling you that you have been randomly selected to win a new iphone or gift card or that you have won the lottery. If you click on them, they take you to a legitimate looking site that asks you for personal information (phone number, banking, address, etc.) to claim the winnings. They are there to harvest your information so they can steal from you.
Fake trending videos	Scammers will post about trending stories with a button to click to see the video. However, when you click on it you will get a message that you need to install a plugin to be able view the video. If you download the 'plugin' you will actually download malicious software.

RECOGNIZING PHISHING ATTACKS

Being observant will usually uncover subtle clues.

Let's look at telltale signs that an email is malicious.

The Giveaway Clues to Phishing Attacks

Most of us have had phishing emails arrive in our mailbox (since about five per cent of all emails are phishing emails), and often they trigger a sense that something is odd about them.

What clues that scammers inadvertently leave in their emails have you noticed?

Spot the Clue

Look at these examples of phishing emails and pick out the clues that indicate it is a phishing email.

Email One

From: PayPal Password [mailto: helpdesk@PayPol.org]
Sent: Thursday, June 11, 2020 2:14 AM
To: person@company.com
Subject: Security Alert

Dear PayPal Customer,

Your password has expired and must be updated, Please click the button below to update your current email account password.

Update Now

Sincerely,

IT- Help Desk

(c) 1999 - 2020 IT- Help Desk

Email Two

.

From: Thank you! Walmart [mailto:thankyou@thankyou.ml]
Sent: Sunday, April 12, 2020 17:01
To: person@company.com
Subject: Claim Your Fifty Dollar Walmart Reward

Your $100 Walmart Gift Card Available

Please Tell us where to send your Gift Card

Grab Your Card Now!

Email Three

Hi Andrew

Someone tried to log into your Amazon account. If this was not you please use the following code to confirm your identity. Please sign in here.

525627

© Amazon 410 Terry Ave N, Geelong, WA, Australia, +68 876 546 143

WHAT CAN A PERSON DO?

Now that you can recognize fraudulent emails, in this session we will look at what you can do to support your company's efforts to prevent an attack.

Supporting Company Efforts

Remember some of the things that companies can do to fight against cyberattacks? These measures are relevant to other cyberattacks as well.

Your company has installed up-to-date firewalls, spam filters, anti-virus software and instituted effective password management with multi-factor authentication and VPN. They have put in place a staff training program and built reporting structures, secure file transfer systems and an effective communication plan.

What can you do to support their efforts?

- Ensure each URL you visit is the real one
- Do not open any email or attachment that seems suspicious or is from someone you do not know
- Be cautious when using Wi-Fi hotspots or non-work internet
- Use strong passwords that you change frequently
- Use two-factor authentication
- Do not use the same password for every device, account or site
- Be sure your antivirus software is up to date on every device you use
- Do not leave your computer unlocked when you are not using it.
- Report suspicious emails to IT

What can you do to prevent an attack?

There are a few ways that you can stop an attack in its tracks. These include:

- Be skeptical about every email you receive, especially unsuspected ones
- Assume that firewalls and anti-virus software do not catch anything
- If you receive an email request that you think might be fake, email directly or call the company to see if the request is real
- Trust your gut feelings
- Check the from address by hovering over it to see who the sender really is
- Be wary about links and attachments – never open one from a sender you do not know
- Hover over a link to check where it is sending you
- Do not follow links to websites embedded in the email – type in correct web address in a browser
- Do not rush – think before you click
- When in doubt call IT help desk with your concerns

Social Media

Individuals can stay safe on social media by:

- Using unique usernames and passwords for each social media account
- Restricting interactions to those they can trust
- Never accept a friend request from someone they do not know
- Not clicking on links (especially if they are asking for personal information) or downloading file attachments
- Knowing what not to post on social media
- Being able to recognize fake accounts (e.g. @Amazom or @Amazon1)
- Noticing grammar mistakes – these are signs of a scammer

Focus on Spear Phishing

As touched on previously, spear phishing is a targeted attack on a company or single individual. Spear phishers are aided by the information we put on our websites and social media, allowing them to personalize their attack. They research to find out names, positions, email addresses, cell phones numbers and more.

These attacks are not as easily recognized as regular phishing scams. They have personalized greetings, great grammar, a sense of familiarity and look very authentic.

Their aim is to gain the target's trust by using their ill-gotten information to make you feel secure with their email, text message or other communication. They send a malicious download link attached to a virus or malware package and wait for you to click on it.

These spear phishers now follow a process to increase the likelihood of success. The steps include:

- Setting a goal (money, information)
- Choosing a target (Accounting clerk, HR Manager, Senior Leader, etc.)
- Doing a background check (using website, social media)
- Developing a personalized attack (based on the target chosen)

How to Protect the Organisation

There are still things you can do to stop the attacker from getting money or information. Many of these approaches are the same as those used for regular phishing attacks, such as:

- Be skeptical about every email you receive, especially unsolicited ones
- Assume that firewalls and anti-virus software do not catch anything
- If you get an email request that you think might be fake email directly or call the company to see if the request is real
- Trust your gut feelings
- Check the from address by hovering over it – see who the sender really is
- Be wary about links and attachments – never open one from a sender you do not know
- Hover over a link to check where it is sending you
- Do not follow links to websites embedded in the email – type in correct web address in a browser
- Do not rush, and think before you click

However, because spear phishing uses information gained from other sources to personalize the phishing attack, there are other things to consider doing, including:

- Consider context, content and the sender
- If you do not know the email sender, check with IT or delete the email.
- If you receive an email from a trusted source with an unusual request, directly message the person (new email, text message, phone call) to verify they were looking for that information