Training – Cybercrime

We often believe that cybercrime only happens to someone else. Maybe we feel we just aren't important enough to be targeted, or perhaps we believe the defense that IT has in place fully protect us. The reality of the situation is - that it just isn't true. In this post, we will introduce you to multiple strategies and attack types the cybercriminals use. Understanding these, will help you identify the risks whenever you're asked to take an action. We will offer you guidance on how you can respond to these threats. Remember these attacks happen way more often than you think - so you need to stay alert and skeptical.

Strategies:

Cybercriminals use certain strategies in their attempts to trick you. Understanding what they are can help you to not get fooled

- **Social Engineering** - Is the art of manipulation, influencing or deceiving you in taking action that isn't in your best interest or in the best interest of your organization. The goal of social engineers is to obtain your trust then exploit that relationship to coach you into either divulging sensitive information about yourself or your organization or giving them access to your network.

- **Malware** – Stands for malicious software. An umbrella term for all the software out there that is being used by cybercriminals to spy on you and steal your information. Oce your computer becomes infected some malicious apps can log all of your keystrokes including your username and password. Some apps take over your computer and can even allow the hacker to turn on your webcam and spy on you or listen to your conversations. Malware attacks often result in data breaches where a bad actor breaks into an organization's network without their knowledge or consent. They steal data or information which is then typically sold to other bad actors for a profit.

- **Disinformation** – Is false information intentionally created to deceive and mislead. This strategy has become more common due to the reach of social media and the ease with which information can be spread via these networks. You and your organization can suffer financial or reputational damage as a result of a successful disinformation campaign. One of the best ways to fight the spread of disinformation is to verify information's truthfulness. Stop and Fact Check before acting upon or sharing information.

- **Pre-Texting** – creates a fictional scenario, where the bad actor pretends they are someone else to gain your trust and get information from you. It can happen in person, on a phone call, through text or email. For example you get a call from someone saying they're from IT and work with Sam who is someone you know. They say they need your username and password to verify a system update. Pretexting scenarios can be very convincing and

these types of attacks are on the rise. It is important to never give information over the phone, in person or online unless you have confirmed the identity of the person who is asking.

The Methods

The methods used by cybercriminals to hack your device and break into your organization's network are referred to as the "Threat landscape". Today's threat landscape is extensive and getting bigger everyday. Whatever device you are using in the office or working remotely - hackers might be trying to use one of the following types of attacks on you. Knowing what they are helps ensure you don't let criminals in.

Three common digital attacks are specifically focused on getting you to take an action that will harm your organization or yourself

Phishing - is the most common digital attack. Fishing is the process in which scammers try to trick you into giving out sensitive information or taking a potentially dangerous action like clicking on a link or downloading an infected attachment. They do this using email disguised as contacts or organizations you trust so that you react without thinking first. For example; you receive an email that looks like it's coming from your IT department telling you that there's a problem with your email account and you need to reset your password. You are asked to click the link in the email. The link takes you to a password reset page with a password field which is what the scammer is after. Once you enter your password, you've given entry into your account. The scammer now has access to your computer and can tunnel into your organization's network. The most effective way you can combat a phishing attempt is to be suspicious of all emails you receive containing links or attachments especially messages that are unexpected.

Spear phishing - is a small focused attack via email on a particular person or organization. The goal is to penetrate your organization's defenses. In this attack the criminals invest time researching a specific target using social media and other open sources of information. Armed with this information they send you a personalized message designed to trick you into taking an action that will put your organization at risk. Spear phishing attacks can be convincing. But just like in any phishing attack you must take an action for it to be effective. One very common form of spear phishing targets top management, typically people who interact with your organization's CEO. A hacker impersonates your CEO and emails you with instructions to do something that could harm the organization. This tactic is called CEO fraud and is growing in popularity. It can even happen via phone with a fake voice message.

Smishing - stands for "short message service SMS fishing, or fishing that occurs through text messaging. For example they send a text message asking you to call a number or click on a link. The message could look like it's from your bank and may even contain most or all of your account number, data usually obtained illegally by hackers. Even if the message you are reading contains your password or your account number it can still be fraudulent

Some cyberattacks launch software that infiltrates your computer or device "behind the scenes" —and can lead to extensive damage to you or your organization.

Ransomware - scrambles the data in computer files making them unreadable. The files are then locked and held hostage until a ransom is paid. Beyond that this malware paralyzes an organization by spreading to all of the devices and files across a network. Hackers increase the pressure on an organization in a variety of ways. A few examples include threatening to increase the ransom amount if you do not pay quickly enough threatening to sell the compromised data unless the ransom is paid. A ransomware attack can be devastating for an organization because of the loss of productivity, reputation, and large amounts of money needed to pay the ransom. Making sure you stop, look, and think before taking an action like clicking on a link, or opening an attachment can potentially prevent this devastation from happening to your organization.

Spyware - is a type of malware that allows hackers to harvest data about you and conduct surveillance on your every move. Although spyware can infect computers and mobile devices, hackers often target your mobile device since it is usually never more than an arms length away. This lets them gather much more information about you, and your organization that they can use. Protect yourself by always being cautious anytime you're asked to install software on your computer or device.

BOT - Cybercriminals have malware that turns your home or office computer into a "bot". A bot is a program that allows your computer to act as a malicious robot for the criminal. It can perform tasks like spewing out spam and fake social media posts attacking other computers or networks, or sending confidential data back to the criminals. These programs can run in the background without your knowledge. Keep a watch out for symptoms like your computer or Internet running really slow or crashing frequently, friends and colleagues getting messages that you didn't send, and pop up windows or advertisements opening even when you aren't using the Internet.

Malicious apps - are another way criminals gain access to your internal network. Imagine receiving a text message with a link letting you know there is an update to one of your favorite apps. It seems super convenient and a good way to get all of the latest features, so you download and install the app, and then your device starts acting funny. What happened? Hackers will hide a malicious program inside an app. Once installed by the user, the hacker can control your devices. Don't let them gain access to your personal information or your organization's network. Protect yourself and your organization by only installing apps from your devices authorized app store and be suspicious anytime an app asks you to grant it additional privileges.

Not all cyberattacks start with an email

Public Wi-Fi - More and more employees are using wireless connections to reach the Internet while working away from the office, coffee shops, libraries and even public parks seem to offer Wi-Fi connections that can be conveniently used to access the organization's network and get work done. Be cautious as these Wi-Fi connections can be unsecured and bad actors want to see what you are doing while online. Never connect to public Wi-Fi unless you are using an organization approved VPN or virtual private network. This technology creates a safe Internet connection that Shields your online activity from criminals.

Fake Profile - another effective trick that criminals use is to create a profile with a bunch of real or fake connections that all look very convincing. For instance the profile could appear to be a headhunter who wants to talk to you about a career move, a potential romantic interest, or someone in your industry who wants you to speak at an upcoming conference. But fake profiles are a growing trend throughout social media and are designed to trick you. So take a close look at any requests that you receive. Some common aspects of a fake profile include model quality or celebrity look alike profile photos in incomplete or generic profile course spelling and or grammar or a suspicious work history. Fake profiles will often lead you on for a while and then send you a link to click on in the message that seems to make sense in the context of the conversation, but this link leads to a site that is able to infect your device with malware. Now the hacker can begin to tunnel into your organization's network

Cyberattacks can also be set into motion in-person or with a simple phone call.

In-Person Social Engineering Attack - an in person social engineering attack is where the hacker walks into your location and tries to hack humans. A classic example is tailgating. This is where the hacker scouts an area like the outside section at your organization and then joins your group, participating in your groups conversation. When your group returns to work, he follows you in just like any other employee and then finds a workstation he can hack and infiltrates your organization's network. Always be alert to those you don't recognize attempting to gain access to areas or devices that they shouldn't be accessing. If you see this taking place report it.

Physical Attack - One highly effective physical attack entirely relies on human curiosity. Hackers typically use flash drives to deliver malware that will infect your device. Attackers leave a flash drive that says payroll where it can be easily found like in your office parking lot, the lobby of your building, or a restroom. Or they could send you an envelope via postal mail with a flash drive inside that looks like it comes from a customer or a vendor. Once someone gets curious enough to plug that flash drive into their computer, that computer is then owned by the bad guys and the organization's network can be compromised.

Vishing - another name for phone based social engineering is voice phishing or vishing. Like phishing, vishing is when the hacker calls you and tries to con you into surrendering confidential information. For example a hacker calls you with a pre recorded message that is supposed to be from a customer support Rep from your bank he says that there's a problem with your account, and asks you to call a fake customer support number to clear things up. The support Rep is part of the con. She will ask for personally identifiable information PII, like your credit card info, pin or other sensitive details. Once she has this information she can access your account and steal your identity and money.

Conclusion: - There's no getting around it. You are a target and the threats we have reviewed happen much more frequently than you realize. This is why it is so important for you to remain cautious. If you receive a suspicious email, text or phone call never taken action or respond to it. Rather contact the organization directly using a customer service phone number listed on their website. You play a central role in protecting your organization against the cyber threats it faces every day. Stay alert to your surroundings and remember to stop, look, and think before taking an action.