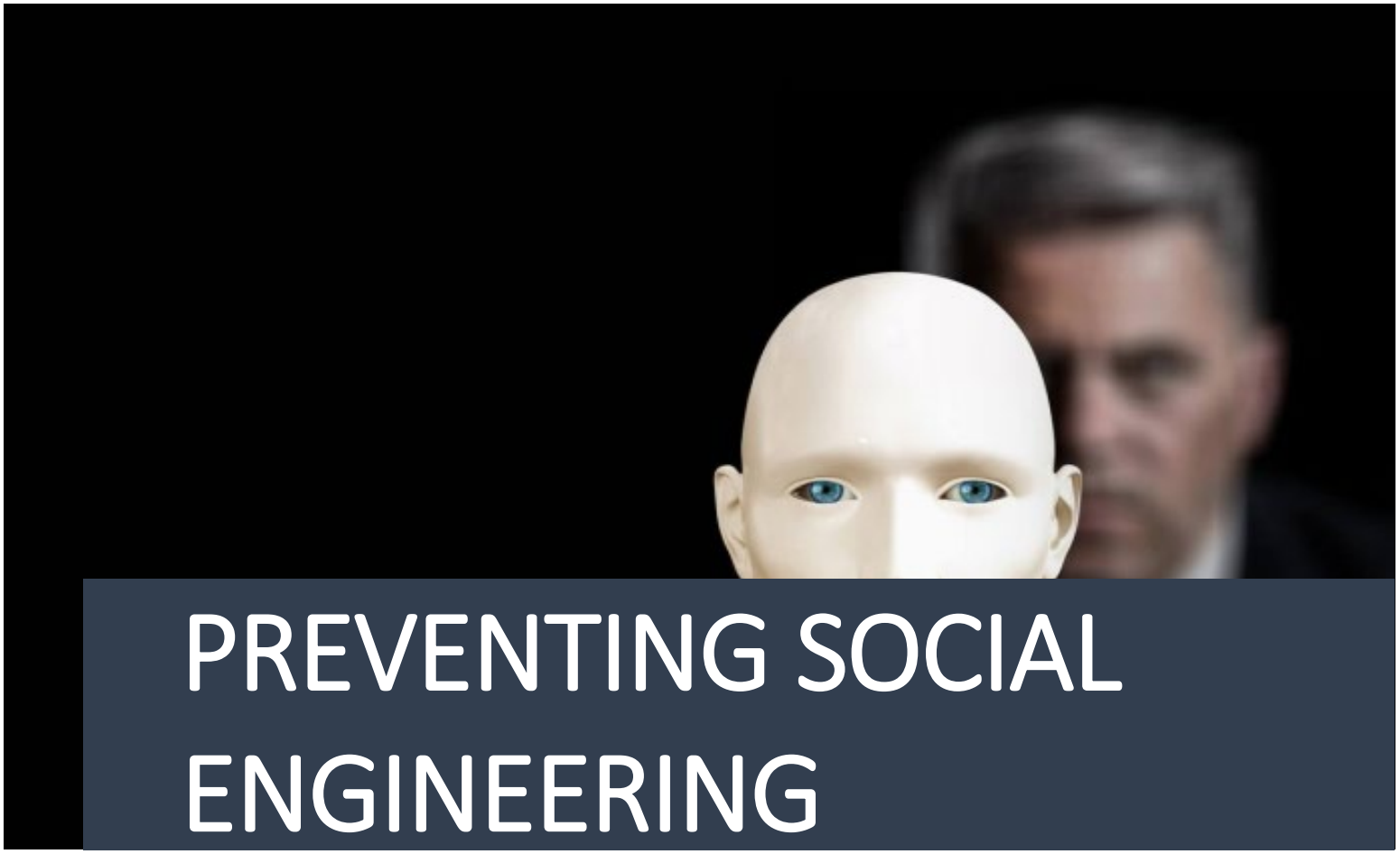


PREVENTING SOCIAL ENGINEERING

Introduction

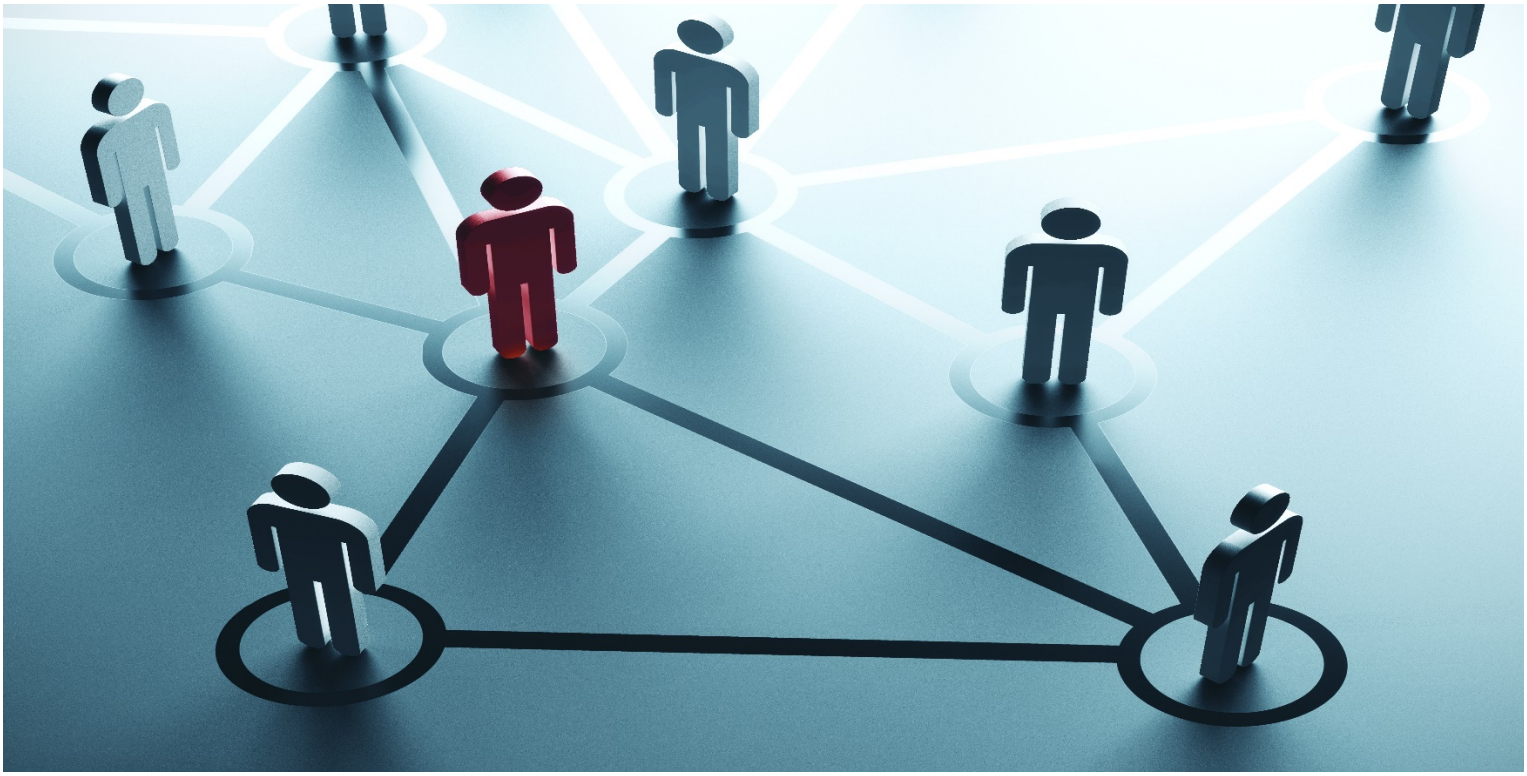
"At its core, social engineering is not a cyber-attack. Instead, social engineering is all about the psychology of persuasion: It targets the mind like your old school grifter on con man." When it comes to cyber-attacks on organizations or individuals, 98% of those attacks rely on social engineering. So, what is social engineering?

When we think about cyber-security, most of us think about defending ourselves against hackers who use technological weaknesses to attack data networks. But there is another way into organizations and networks, and that's taking advantage of human weakness. This is known as social engineering, which involves tricking someone into divulging information or enabling access to data networks.

There are several types of social engineering attacks. So, it's important to understand the definition of social engineering, as well as, how it works. Once the basic modus operandi is understood, it's much easier to spot these attacks.

Social engineering attacks can be particularly difficult to counter because they're expressly designed to play on natural human characteristics, such as curiosity, respect for authority, and the desire to help one's friends.

Put simply, social engineering is the use of deception to manipulate individuals into enabling access or divulging information or data, but armed with knowledge, you can protect yourself.



Common Types of Social Engineering Attacks

Social engineering attacks are diverse with each subset of attacks having their own subsets of attacks. To better protect yourself, its critical to understand the common tactics that can be used against you.

Phishing

This is the most well-known type of social engineering attack. There are many subsets of phishing attacks, but they all have one goal in mind: compromise your data. Phishing attacks use email, phone calls, and SMS/text messages to deceive an individual into divulging sensitive information. Common phishing attacks are vishing, smishing, spear phishing, whaling, impersonation, and clone phishing.

Scareware

Scareware attacks use pop-ups and/or ads to scare people into visiting a malicious website, install malware onto their devices, contact the attacker, or send money to the attacker. Common examples include fake virus popups, fake tech support, malvertising, and law enforcement scams.

Tailgating & Shoulder-Surfing

Tailgating involves an unauthorized person closely following another authorized person into a secured area. This can also involve waiting for a person to leave their computer unattended, but logged in. This commonly occurs due to kindness and ignorance, respectively.

Shoulder-surfing involves an attacker discretely observing a user accessing or typing sensitive information.

Deep Faking

Advancements in AI have granted attackers access to the most sophisticated type of social engineering attack we've seen thus far. AI now allows attackers to mimic voices, swap faces, and even create fake videos. Though this used to be uncommon, these types of technology have become more accessible and usable for the public. Attackers have already successfully used deep faking to extort millions on dollars.

Baiting

Baiting is a tactic in which an attacker uses a trap or bait to trick an individual into installing malware or divulging sensitive information. The most common baiting tactic is leaving a malicious USB somewhere unattended in the hopes that a person will plug in the USB to see what is inside. These USBs may have software that can automatically run and compromise a device and the network.

Honeytrap

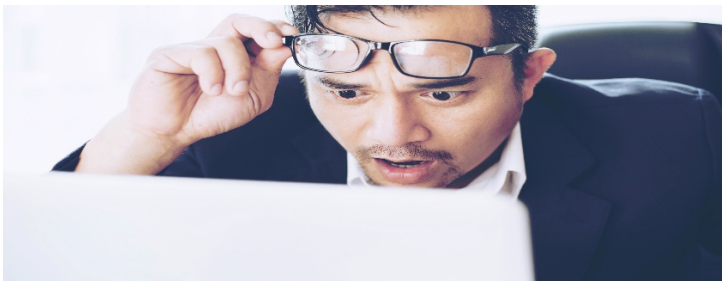
A honey trap is an attack where the social engineer assumes the identity of an attractive person. They then lure the target into false relationships to eventually steal money or their sensitive information. This is commonly used in social media such as e-dating services.

Psychology of Social Engineering

Social engineering at its core is the manipulation of trust. If we were to create an equation that determines our trust, A+B+C+D+E+F+G = Trust, social engineers work the variables that dictate trust by plugging in varying values that affect our sense of fear, authority, reciprocity, urgency, consensus, connection, scarcity, and consistency. To prevent these attackers from solving the equation, it is crucial to understand the aspects of human behavior that can be manipulated.

Authority

Attackers understand people are naturally inclined to trust and follow authority. Whether it's a lawyer, professor, police officer, or significant other, these types of individuals command respect and trust. This trust can be easily manipulated. By impersonating someone of authority, attackers put themselves in a strong position to successfully exploit their target.

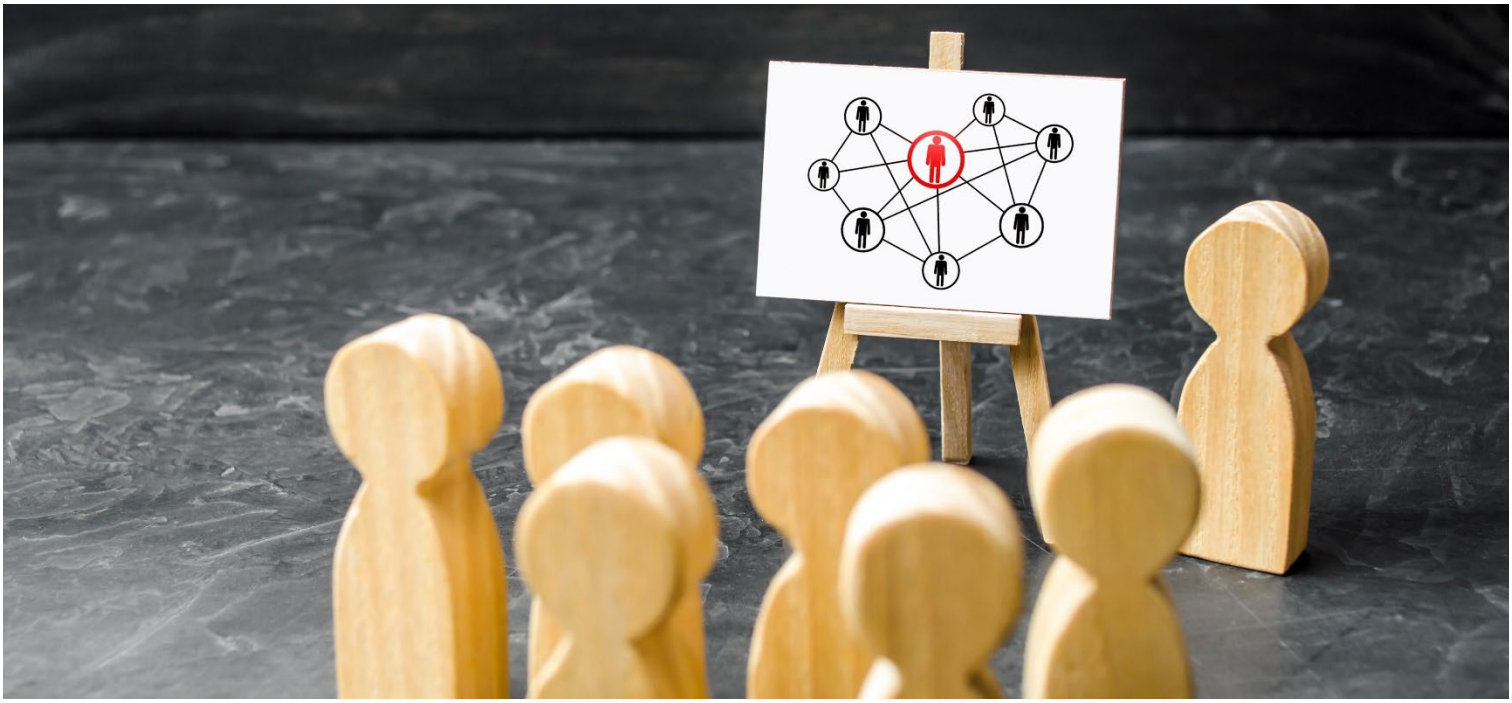


Reciprocity

When someone does something nice for you, there's a tendency to want to repay the kindness. Cybercriminals exploit this instinct by offering something small, like a gift card, to gain your trust. Once you've accepted their "gift," you might feel more obligated to follow through on their request, such handing over some information.

Urgency

“Fight or flight” responses are meant to protect us, but attackers see the latter as a powerful tool. Often used with authority, attackers will attempt to pressure the target with fear, causing them to act without considering the consequences.



Consensus

This concept is grounded in the social norm that individuals tend to act based on what they perceive others would or have. Attackers may exploit this by claiming that your coworker has already clicked this link to complete the survey last week or flooding a malicious website with fake testimonials suggesting legitimacy.

Connection

We're naturally more receptive to people we like or share a rapport with. Shared interests, compliments, and cooperation strengthen this sense of connection. The more we feel a connection with someone, the more likely we are to lower our defenses. Attackers exploit this feeling by either building a relationship with you or impersonating someone you already trust.

Scarcity

Scarcity, often combined with urgency, is a widely used marketing trick—when something seems limited, people are more likely to believe it's valuable or worth acting on. Attackers utilize scarcity by claiming that a product is running out or only available for a short time. This sense of urgency drives targets to quickly click on a malicious link before they "miss out" on the opportunity.

Consistency

With integrity in mind, people generally strive to be consistent with their actions and commitments. Studies show that once someone makes a small commitment, they are more likely to stick to it. Attackers exploit this by having you agree to something minor, only to follow up with a larger request, hoping your sense of consistency will lead you to comply.

Preventing Social Engineering

Now that you understand the common types of social engineering attacks and the psychology behind them, you can more easily recognize and prevent them. Here are some tips to identify and stop social engineers in their tracks.

Patience Is a Virtue

Attackers often rely on psychological tactics to manipulate targets into making decisions without evaluation. It's important to cultivate a mindset that is patient. This grants you time to evaluate the situation, review the details, and then make a well-informed decision. It is rare that you don't have the time to consider the situation, despite what others may say. Whether it is an email, phone call, text message, or in-person talk, take a pause and ask yourself questions like below:

- Is the language used trying to appeal to an emotion? Is it driving a sense of urgency or are they building a connection? If there is a connection, is there a request that follows soon after?
- Should this person be sending me something? Is that the correct sender or caller? Why is this person requesting something and at this time?
- Is this link malicious? Is this attachment malicious?

Taking the time to ask yourself questions and thinking through the answer will help you create a strong defense against social engineers.

Check the Source and Content

Take a moment to think about where the communication is coming from and what is in that communication; do not trust it blindly. A USB stick turns up on your desk and you do not know what it is. An out of the blue phone call says you've inherited $5 million. An email from your CEO asking you to buy gift cards at 3 AM. Your CEO video calls you saying you must transfer funds immediately. These sound suspicious and should be treated as such. Consider the following tips for each scenario.

For Emails and Messages:

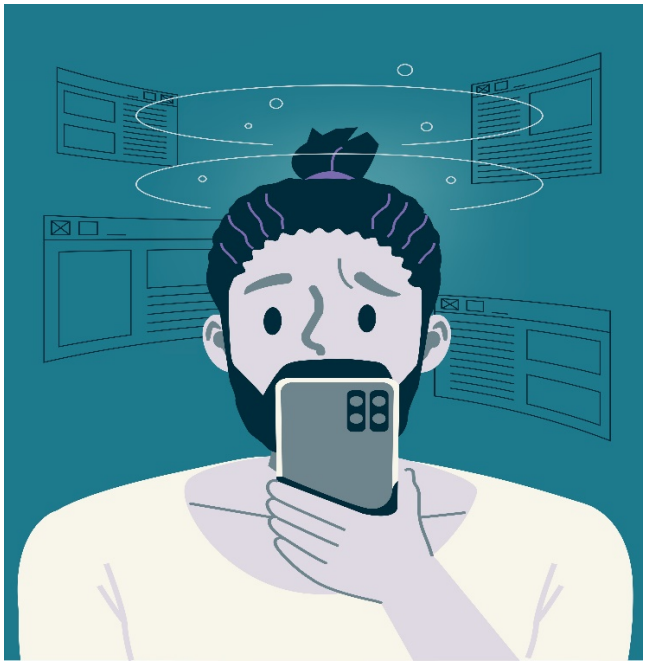
- Look at the email header, sender name, or phone number for sender information.
- Review the content for typos, errors, vagueness, psychological manipulation, and incorrect alerts.
- Hover over hyperlinks, scan the attachments, and preview QR code links.
- Consider the context of message, such as the time of receipt, sender information, whether you're expecting this message and/or the links/attachments in the message.
- To be safe, contact the person the sender claims to be through a confirmed legitimate number such as on an official website.

For In-Person:

- Do not allow others to tailgate you into a secured area.
- Lock your devices if you need to leave them unattended.
- Listen for psychological tactics.
- Do not plug in any unknown devices into your own device.
- Store and dispose of sensitive properly
- Before accessing sensitive data, be sure only authorized personnel can view it.

For Callers:

- Check to see if the caller number is correct. However, remember hackers can spoof the phone number.
- Listen to see if the caller is utilizing psychological tactics.
- Consider the context of the call, such as the time of call, caller information, and if the content of the call makes sense.
- Test for AI voice replication by having the caller replicate emotions, watch for delays in responses, and whether they can be interrupted.
- Test for AI video replication and face swapping by having the caller move their head around in wide motions, looking for clipping or distortions, and watching for correct lighting.
- To be safe, hang up and go to the official website and get in contact with an official representative, as they will be able to confirm if the email/message is official or fake.



Secure Your Devices

It's also important to secure devices so that a social engineering attack, even if successful, is limited in what it can achieve. The basic principles are the same, whether it's a smartphone, a basic home network or a major enterprise system.

- **Keep your anti-malware and anti-virus software up to date.** This can help prevent malware that comes through phishing emails from installing itself. Use a package like Kaspersky's Antivirus to keep your network and data secure.
- **Keep software and firmware regularly updated**, particularly security patches.
- **Don't run your phone rooted, or your network or PC in administrator mode.** Even if a social engineering attack gets your user password for your "user" account, it won't let them reconfigure your system or install software on it.
- **Don't use the same password for different accounts**. If a social engineering attack gets the password for your social media account, you don't want them to be able to unlock all of your other accounts too.
- **Use multi-factor authentication (MFA)** so that just having your password isn't enough to access the account. That might involve voice recognition, use of a security device, fingerprinting, or SMS confirmation codes.
- **If you just gave away your password to an account** and think you may have been "engineered," change the password right away.
- **Keep yourself informed about new cybersecurity risks** by becoming a regular reader of our Resource Center. You'll then know all about new methods of attack as they emerge, making you much less likely to become a victim

Think About Your Digital Footprint

You might also want to give some thought to your digital footprint. Over-sharing personal information online, such as through social media, can help attackers. For instance, many banks have “name of your first pet” as a possible security question — did you share that on Facebook? If so, you could be vulnerable! In addition, some social engineering attacks will try to gain credibility by referring to recent events you may have shared on social networks.

We recommend you turn your social media settings to “friends only” and be careful what you share. You don't need to be paranoid, just be careful.

Think about other aspects of your life that you share online. If you have an online resumé, for instance, you should consider redacting your address, phone number and date of birth - all useful information for anyone planning a social engineering attack. While some social engineering attacks don't engage the victim deeply, others are meticulously prepared - give these criminals less information to work with.

Social engineering is very dangerous because it takes perfectly normal situations and manipulates them for malicious ends. However, by being fully aware of how it works, and taking basic precautions, you'll be far less likely to become a victim of social engineering.

Closing Tips

By following the rules below, you can ensure that you are creating a security-conscious culture at work and home.

- Take your time to review the details of an interaction or message before acting.
- Be suspicious of unsolicited phone calls, visits, or individuals asking about employees or other internal information.
- Be conscious of psychological manipulation tactics.
- Do not provide personal information or information about your organization, including its structures or networks unless you have confirmed it is needed and the recipient is legitimate.
- Do not reveal personal or financial information in an email. If you plan to send this information, make sure it's encrypted.
- Be conscious of your digital footprint. The information you put out to the world can be used against you.
- If you must send sensitive information over the Internet, always check a website's security. Ensure the URLs begin with an "https," which indicates a secure site, not an "HTTP."
- Always use MFA, although some may see it as a nuisance. MFA adds an extra layer of security, ensuring that the person signing in is the one authorized to sign in.
- If you are unsure whether an email or message is legitimate, look at the markers of illegitimacy such as headers, errors and typos, false hyper-links, etc.
- When in doubt, look to contact the sender or caller through information listed on official documentation or websites outside of the original call, email, or message.
- Keep your devices updated and ensure that anti-malware software is installed.
- Shred or dispose of properly any documentation that may contain Personally Identifiable Information (PII) or Personal Health Information (PHI), such as addresses, SSNs, and other personal information that is not public knowledge.

Maintaining a security-conscious culture where security is ingrained in daily practices enhances resilience against malicious tactics and cultivates a proactive mindset to cybersecurity in the workplace and at home.