SecurityAwarenessNews

the security awareness newsletter for security aware people

Fundamentals of Security Awareness

Top 5 Fundamentals of Security Awareness

What Happens
When You Click on A Phishing Link?

Security by Design and Default

Top 5 Fundamentals of Security Awareness

Finding success in sports, gaming, and various hobbies always starts with learning the fundamentals. Before a basketball player can be an effective player, they must first learn how to dribble. A golfer must perfect their swing before stepping foot on the course. A chess player needs to know how and when to sacrifice or leverage a pawn.

Security awareness also begins with fundamentals. And while we could list dozens of action items relevant to privacy, these five fundamentals stand out as the building blocks.

Identifying Phishing Attacks

Still the most common element of "how people get hacked" stories, phishing remains a top threat facing organizations in every industry.

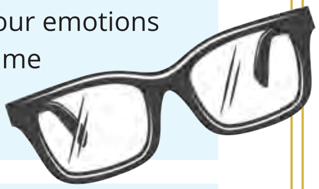
Learn to spot these attacks by familiarizing yourself with typical red flags, such as poor spelling and grammar, threatening or urgent language, and unexpected links or attachments. Stay alert, and think before you click.

Thinking Like Scammers

Like the red flags of a phishing email, getting to know a scammer's thought process will help you identify when you're being targeted.

For example, they may email or call you pretending to be a member of our organization who needs your login credentials. They may approach you in person and ask you to allow them physical access to a secured area. They may use fear tactics such as threatening messages claiming an account has been compromised.

In all cases, scammers want to use your emotions against you. Don't fall for it! Never assume someone is who they say they are, and think critically in every situation.



Creating Strong Passwords

Your online privacy is only as strong as the passwords you create. Here at work, it's your responsibility to know and follow our current password policies. In your personal life, protect your accounts with these quick password tips:

- ***Use at least 16 characters – length equals strength! The shorter the password, the easier it is to crack.***
- ***Create passphrases – a passphrase contains a string of words that is easy for you to remember yet hard for others to guess, such as a random quote from your favorite song or book.***
- ***Be unique – never use the same password twice. Every account deserves its own strong password or passphrase.***

Reporting Incidents

If you fail to report security incidents or don't report them promptly, you prevent our organization from effectively mitigating the threats they pose.

Following Policy

We designed our security policies to protect the privacy of our employees, clients, customers, and business associates. By always following policy, you help our organization maintain that privacy.

Security

by Design and Default

In the software development world, programmers are encouraged to build applications with "security by design." Meaning, security is a forethought in the design process, and the product builds on that forethought from the ground up. It's a fundamental measure ensuring that security receives priority at every point in the application's lifecycle.

Similarly, "security by default" means releasing a product to the public with security settings maxed out. Imagine a social media app that defaults with your account set to fully private. No one else can see your profile, pictures, status updates, and so on, until you electively change those settings.

These two concepts share a common goal: protecting the privacy of everyone who uses the product. Let's explore how we can apply them to our processes here at work.

For example, when you receive an email with links or attachments, you should handle that email with security as the forethought. By default, you should remain skeptical and assume those links or attachments can't be trusted.

When you access confidential data, you should, by default, do so with the understanding that a small mistake could yield significant consequences. Even something as simple as emailing the wrong person creates the potential for a data breach.

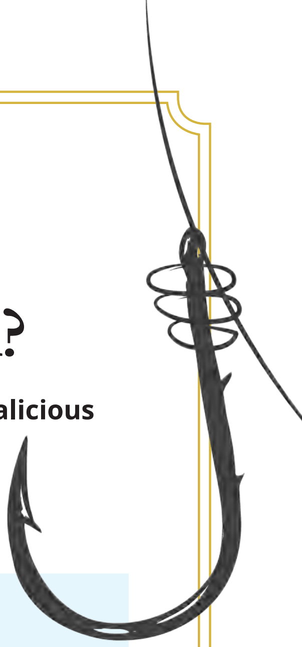
If you find a USB flash drive or notice the door to a secured area left open, your instincts should be designed to presume something is wrong and that you should report the incident immediately.

By making security awareness a default part of your day-to-day functions, you automatically help our organization identify threats and reduce risks. Likewise, our organization's policies were designed to ensure that the confidential information entrusted to us remains confidential. And by default, you are required to always follow those policies.

Remember, the goal of security by design and default is to protect the privacy of everyone. And even though most of us aren't software designers, we can still borrow these concepts and use them to improve our overall security posture.

What Happens

When You Click on A Phishing Link?



A cornerstone of cybersecurity is not clicking on phishing links or downloading malicious attachments. But what happens if you do? Here are a few potential consequences:

1 You become a high-profile target.

By clicking on a phishing link, you confirm for the attacker that 1) you're a real person, and your email is current, and 2) you're gullible. The attacker might use this information to build a profile about you and sell it to other attackers, who will then send much more threatening phishing emails. You could also experience a major increase in spam.

2 You have personal information stolen.

In a lot of cases, a phishing link will direct you to a webpage that looks legitimate. The page will ask you to enter various types of personal information like your full name, email, username, password, and so on. If you proceed, you effectively hand over your identity to a criminal, who can use this information to open fraudulent accounts in your name.

3 You lose control of your accounts.

Let's say you're logged into your bank account when you click on a phishing link. This may allow cybercriminals to run an exploit known as session hijacking. Meaning, they could intercept the communication between the bank's website and your computer and take control of your account. If successful, they will now have all the same access you have, allowing them to transfer money, change passwords, and steal personal data.

4 You infect your device with malware.

In more insidious phishing attacks, clicking on a link or downloading an attachment could result in malicious code that corrupts your device, steals data or, worse yet, infects your computer with ransomware. Ransomware is of particular concern here at work because it could encrypt our data or lock our systems until a ransom is paid, leading to both a loss in revenue and expensive downtime.

All of these scenarios are just examples of what could happen. Regardless of severity, falling for a phishing scam must be avoided no matter what. Remember, cybercriminals often cast wide nets with generic phishing emails that feature the typical, easy-to-spot red flags. But some attacks are much more sophisticated and may appear to come from someone you know, such as a co-worker or manager.

Use extreme caution when handling messages (including those on mobile devices) that contain links, attachments, and requests for information or money. As a rule, if you're unsure, don't click! And report all phishing attacks immediately.