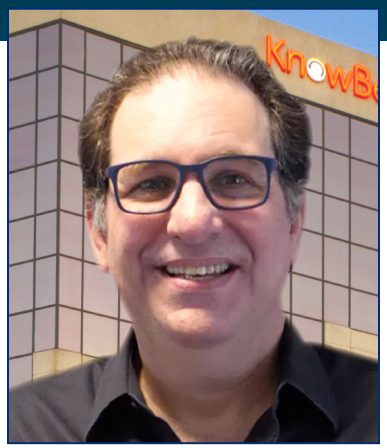
Kevin Mitnick Security Awareness Training

Don't Become a Victim!



Cybercrime is big business—and happens more often than you think! Be aware of the tactics and attacks hackers use on YOU.

Kevin Mitnick, "The World's Most Famous Hacker" and KnowBe4's Chief Hacking Officer, will provide you with information about cyberthreats, as well as the key takeaways that can help minimize the risks you and your organization face.

TACTICS

Information Gathering

Social media is a gold mine of information hackers can use to trick you and your co-workers. Each piece of additional information gathered increases their odds for a successful attack. Some examples of things you should never share are travel plans, your organization's internal processes, or less obvious pieces of information like reports, financial information, or even the software your organization uses.

Takeaways: Be careful what you share. Ask yourself if the information you're about to post will be useful in conning you or your co-workers. Make sure you're familiar with your organization's expectations regarding what and how much you can share on social media by following your organization's social media policy.

Fake Profiles

Hackers use the information readily available through social media and online search engines to create an online persona that gets your attention. Their goal is to gain your trust and get you to take an action, like opening an attachment, clicking on a link, sending money, or giving them information to make their next attack more successful.

Takeaways: Never assume the security settings on social media sites will keep you safe from a fake profile attack. Be wary anytime you are asked to take an action on any site.

Disinformation

This is where hackers create and distribute false information to manipulate your thoughts and actions and cause damage to you or your organization. This strategy has become more common because of how fast information travels across social media networks.

Takeaways: Anything that tugs at your emotions is a warning sign. Always fight the spread of disinformation by verifying information's truthfulness. Stop and fact-check before acting upon or sharing information.

ATTACKS

Physical

Hackers might try to steal information using physical access. They might "tailgate" you or one of your co-workers, which is when they will act like they work there and follow you into the office. They might also use a uniform or stolen key card to get access to unlocked workstations or valuable information left out on desks.

Takeaways: Stay aware of your surroundings. Don't let anyone you don't know in. Always lock your devices when they're not in use, even if you're stepping away for a moment. Also, adopt a clean desk policy, which means keeping important items locked away when not in use.

Phishing

This is the method most often used by hackers. They use emails disguised as contacts or organizations you trust so that you react without thinking first. Their goal is to trick you into giving out sensitive information (i.e., your username and password), or taking a potentially dangerous action (i.e. clicking on a link or downloading/opening an infected attachment).

Takeaways: Phishing attacks are the most common type of attack because of how effective they are. Hackers are really creative when they target you, and it can be very difficult to tell if a message is real or fake. Stop, look, and think before you click that link, open that attachment, or share sensitive information.

Pretexting

Hackers sometimes use a made-up scenario to gain your trust so they can get the information they want. For example, they'll call and pretend to be on your IT team, mentioning the names of individuals they found while researching your organization. Then, they will say some updates just rolled out, and they need to validate a few things on your workstation.

Takeaways: Since this attack is convincing and prevalent, be vigilant. Never give information over the phone, in person, or online unless you've confirmed the identity of the person asking. You can do this by calling the person back using a verified phone number, on the organization's phone directory or main website.

Wireless Connections

More and more organizations are allowing their employees to work in places away from the actual office. Coffee shops, libraries, and even public parks often offer Wi-Fi connections that can be conveniently used to connect to the office as well as the internet. Be cautious as these Wi-Fi connections can be unsecure, and hackers want to see what you are doing online.

Takeaways: 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.

Cybercrime Happens Way More Than You Think!

The cybercrimes you hear about on the news are just the tip of the iceberg. In fact, one happens every 36 seconds!

Here are some facts about the scale of increased cybercrime:

2,244
Cyberattacks per day, according to the University of Maryland!

37%
Month-to-month increase in cyberattacks due to COVID-19 pandemic!

$108M
Lost to scams in a recent 6-month period.

KnowBe4