Blog for MPA Networks

https://www.mpa.com/blog.aspx?p=fake-phishing-the-ultimate-security-training

Fake Phishing: The Ultimate Security Training?

Posted January 5, 2016

What is the current state of your company's IT security training program—if you have one? Many companies settle for an annual group training session to broadly review the major types of cyber-threats—viruses, malware, and phishing.

The problem with once-a-year "standardized" training is that once employees go through it the first time, they may not fully pay attention in the future, thinking they've "heard it all before." That's when they're most vulnerable.

"It Won't Happen To Me"—Until It Does

Recently, a friend of ours—who normally prides himself on being "smarter than the average bear" when it comes to **computer hygiene**—confessed he finally got duped into downloading malware directly to his desktop PC. He tried updating to the latest version of CCleaner, a popular, trusted freeware utility which removes temporary files, cookies, and other unwanted clutter from a hard drive. But the page he was directed to had *two* different "Download" buttons… and he clicked the wrong one. After ignoring dire warning screens from his anti-virus program ("It's only CCleaner," he reasoned), he discovered he'd actually just downloaded *several* unfamiliar programs, masquerading as system processes in his Windows "Task Manager."

The first consequence: an uncloseable pop-up window requesting payment to remove multiple "detected threats" (which he of course declined to pay). Fortunately, he immediately deleted all the "scamware"—via several malware-removal apps—before hackers could unleash more havoc. He was reminded to stay *reasonably* skeptical of almost everything online—and to never again let his guard down.

Time For Some "Tough Love"?

You can warn someone of looming cyber-dangers until they're tired of hearing it… but sometimes the best education is simply "learning the hard way." A handful of security contractors are helping companies actually test their employees by providing ***fake* phishing emails**—which mimic the sophisticated tactics of genuine scams (offering bogus apps, phony "updates," and more). When they click on a deceptive link, they're quickly informed they've dodged a bullet:

"Oops! You've just fallen for a fake phishing email test. Luckily, your computer remains unharmed for now, but keep in mind this is how hackers regularly trick victims into compromising network security..."

One strong proponent of fake phishing is the Department of Homeland Security—which recommends federal employees who repeatedly fail such tests should have their security clearances revoked.

The point of fake phishing tests isn't to anger or shame employees who unwittingly take the bait. **The goal is to prove that cyber-threats are definitely real, and they should take security very seriously.** Nobody wants to be the *real* victim. For management, the overall "conversion rate" of a fake phishing test is a true metric of an IT security training program. If too many employees allow themselves to be conned by a simulated phishing scam, their existing training isn't working.

For more ways to boost security measures within your business, get in touch with a local MSP.