You Can Stop Cyber Crime!

It use to be that phishing email messages were easy to spot: they were from an unknown person, full of typos and grammatical errors, and often used broken English. They sometimes included a sob story that was truly not believable.

Not anymore. The hackers are becoming more clever and using actual logos (or very good renditions of them), have better language skills, and are making the messages appear to come from a friend or colleague. These make it very difficult to detect fact from fiction.

But there is hope! Fraud attempts can be identified with training and education, which will lead to less exposure and risk.

Training Programs

A good training program is not difficult to set up. If it's not reasonable to do it yourself, there are many organizations that provide this service and there is one for every budget. They should include information on identifying phishing, and instruction on what to do if someone accidentally executes malware. Test employees and anyone who connects to your network. Yearly is not enough, quarterly is recommended, and if you can do it more often, do so! Small- to medium-sized companies are becoming targets of choice. Taking some time to implement good security practices can do wonders to lower your risk.

Tips and Advice

- **Watch for subtleties such as the way the email is written.** If someone wouldn't use a word of phrase in a particular way, question it. There is a recent example of an attacker requesting a wire transfer, but was thwarted because the attacker used the word "please" in the message to the accountant. This was apparently not normal for that executive.
- **For those in charge of protecting networks, implement defenses.** Having firewalls in place at the perimeter is mandatory, but those can be vulnerable, too. Take the next step and segment the internal network. If there is a reason to seat people in different areas, perhaps it makes sense to separate the networks, too. If a virus gets into one area, it will more likely be contained long enough to address it.
- **Put a patch policy in place.** This is something that may seem elementary, but it is often overlooked. Keeping all devices updated with security and critical patches is paramount. A Google® study found that companies largely fail to put patching and updating systems at the top of the priority list. This can significantly lower your risk.
- **Don't forget to include devices that are serviced by outside vendors in the patch program.** Often, these machines such as camera systems and card access systems don't get attention for long periods of time. Put in contracts that regular patching takes place.

Get the lastest information from our website. Scan the QR Code to go directly to this page.