Trustmark

SECURITY WATCH NEWSLETTER

Vol. 5, Number 4

Smart People Fall Victim to Scams Too

Individuals and organizations spend a small fortune purchasing technology and security services, but their computers and confidential information could remain vulnerable to old-fashioned human manipulation, i.e. scams.

Smart people fall victim to scams every day. Scams succeed because they look like the real thing or try to take advantage of a busy individual or an active business environment. Even when only a small percentage of targets are deceived, scamming is still a billion-dollar industry.

Email scams have been going on for years and remain effective because both individuals and businesses rely heavily on email and instant message tools.

Scammers take advantage of the good names of reputable online companies and spoof their email addresses, logos, and links. It's easy to copy letterheads, names and logos to make them look real, and it's simple to create phony websites, use fake credit cards or checks and obtain business details such as your name and address through public listings or from your website.

The most common scamming technique is to send an email to thousands of online users asking them to re-enter or update their personal information under the pretext that their "account is about to expire" or "multiple log-ins have been detected" or they've "just won the lottery."

How to protect yourself

Trust your instincts. If you don't feel comfortable dealing with a particular company or individual, or if you feel pressured to take action immediately, maybe you shouldn't. The single most important key to avoid being taken advantage of is to not give sensitive information to anyone unless you can verify that they are who they claim to be and that they have a legitimate need for access to the information.

Next Steps

If you think you've become a victim of a scam, contact the company being impersonated and ask them to open an investigation. Also, file a complaint with the following:

- The Federal Trade Commission at www.ftc.gov/complaint
- Your state Attorney General at www.naag.org
- Your county or state consumer protection agency. Search "Where to File a Complaint" at www.consumeraction.gov
- The Better Business Bureau at www.bbb.org

Five Simple Ways Your Business Can Avoid Cybercrime

Private businesses across the nation are adopting a variety of measures to defend their networks and sensitive data against attacks like the ones experienced at major retailers last December.

A layered security approach, in which multiple forms of protection are integrated for maximum security, is the best way to safeguard against cybercrime. Another defense is to be aware of the threats and create security policies to deal with them. Employing the following low-tech, common sense actions can help seal up vulnerabilities at little or no cost.

1. **Update software.** Cybercriminals take advantage of vulnerabilities, so make sure software and antivirus/antimalware programs are intended for business use, and are patched and up-to-date.
2. **Employ stringent password policies.** Use a mix of alpha and numeric characters that do not resemble words, and be sure to use different passwords to access accounts and programs.
3. **Limit access to financial data.** Use a computer that is dedicated as a banking terminal, dual authentication, and positive pay, where the bank is provided a list of authorized payments through a separate channel. Also, limit the number of people who have log-in credentials to financial data.
4. **Educate employees.** Train employees on safe workplace email and Internet usage. Preventing behaviors that put a system at risk is very important.
5. **Perform an automated vulnerability audit scan.** If you can't afford to hire consultants, you probably can afford a one-time, automated scan of your network. There are many vulnerability management products on the market at all price points. Regular use of them should be part of your network maintenance routine.

These countermeasures can go a long way in mitigating your risk and protecting your data. But they are only a sampling of the steps that a diligent IT administrator could implement to increase network security.

Trustmark National Bank
Offices in Alabama, Florida, Mississippi, Tennessee & Texas