{e}mazzanti® technologies
TECHNOLOGY STRATEGIES FOR BUSINESS GROWTH.

Gone Phishing: How to Be Safe from Personalized Spear Phishing Attacks

Phishing attacks entered the scene when AOL still ruled the Internet. More than two decades later, cyber criminals continue to use targeted phishing techniques for one simple reason. They work. Specialized attacks, known as spear phishing, use personal details to trick victims into clicking malicious links or sending sensitive information.

For example, last year, hackers compromised the email system for an Ohio parish. After spying on email conversations, they posed as a construction company hired to complete parish renovations. Soon, the parish received an email, supposedly from the contractor, listing new instructions for payment transfer. In response, they paid nearly $2 million to a fake account.

Similar attacks have cost businesses and individuals millions of dollars. Even Google, Amazon and Facebook have fallen victim. And, while the attacks often involve requests for money, cyber criminals also use spear phishing to deploy malware and steal trade secrets or login credentials.

Understand the Spear Phishing Process

As in any war, understanding how your opponent operates will prepare you to mount an effective defense. In spear phishing, hackers first identify a target. Unlike basic phishing, which casts a wide net, spear phishing **focuses on a specific person or group**.

> *This personalization requires more effort, but it gives criminals a high degree of success.*

Once the attackers have chosen a target, they **study their prey** by combing through social media and other online information. With minimal effort, attackers can learn a surprising amount. For example, they can discover where you live and work, who your friends are, the details of your latest vacation and even your recent purchases.

Armed with personal details, hackers customize an email, text or phone message. Typically, they **pose as a trusted source**, such as a legitimate business or a coworker. The content of the message includes specific details and most likely conveys a sense of urgency.

Finally, the attacker **disguises the message** so that it appears to come from a known sender. Unfortunately, cyber criminals have become quite proficient at spoofing emails or cell numbers. They may send from an email address nearly identical to a legitimate address, or they may actually take over a real account.

Tips to Avoid Becoming a Victim

Cyber criminals will keep phishing, and they will use increasingly sophisticated tools to do so. But you can protect yourself from falling victim to most scams by following some common-sense tips.

1. **Watch what you post online** – Avoid the tendency to overshare on social media. In particular, never post your phone number or email address. Also, adjust your privacy settings to limit who can see your posts and help protect your digital footprint. To play it safe, assume that bad actors can view anything you post on the internet.

2. **Use smart passwords** – Never re-use passwords or password variations. Once hackers obtain a password, they will try it on multiple sites. To be safe, use unique passwords, preferably phrases or random combinations of letters and numbers.

3. **Know common phishing techniques** – Spear phishing emails generally use terms like "urgent," "invoice due," or "request." Common subject lines refer to financial items and payments. The messages often include attachments or ask you to click a link to enter required information.

4. **Never click an unexpected link or attachment** – Security experts have repeated this warning over and over again. And yet, users keep clicking links and opening attached files, opening the door for malware. In particular, never click a link that seems to come from a bank or other business. Instead, go directly to their official website.

5. **Verify a request before entering information** – Even if an email includes personal details or seems to come from a trusted source, confirm the request through alternate channels before complying. For example, if you receive an email from your boss asking for sensitive information, call her to verify that she did, indeed, send the email.

Partner with a Trusted Security Expert

Because spear phishing uses customization so effectively, it can prove difficult to spot. Strengthen your defenses with a comprehensive security strategy. eMazzanti provides a full suite of cyber security solutions designed to address threats on multiple levels. Protect your business with world-class firewalls, network security, 24/7 monitoring and more.