SMALL BUSINESS CYBERSECURITY CORNER

Phishing

You were just going about your day, managing your small business when you realize you can no longer log in to your bank account. Did you forget your password or has someone changed the log in, effectively blocking you from your own money? Were you "phished"?

What is "Phishing"?

A sneaky cybercriminal sends you an email with graphics and fonts that make it appear to come from your bank. The email claims something is very wrong with your account, and they need you to log in and fix the problem immediately. They helpfully include a login link in the email and you're about to click - when you remember, this might be a phishing attack! A phishing attack is an attempt by criminals to trick you into sharing information or taking an action that gives them access to your accounts, your computer, or even your network. It's no coincidence the name of these kinds of attacks sounds like fishing. The attack will lure you in, using some kind of bait to fool you into making a mistake. Phishing attacks may strike using your email, text messages, or websites to trick you by posing as a trusted person or organization. You might get a text or email from someone you know or an organization you trust, requesting you click a link or download a file. Usually there's a sense of urgency or a problem you need to resolve.

In this animated story, a business manager receives an urgent email from what she believes to be her bank. Before she clicks an included web link, a business colleague alerts her to possible harm from a phishing attack. Learn about common types of phishing messages and why any business owner or employee needs to be vigilant against their danger. This video also helps the viewer learn how to stay prepared, get helpful information, and find support from NIST's Small Business Cybersecurity Corner website.

When you click the link or download the file, you can unwittingly install programs that provide the attacker with access to your computer or even your entire network. Clicking the link might also take you to a fake login page for a website you trust. Any passwords you enter will be captured by the attacker.

Some attackers time their attacks for seasonal issues like tax season or the holidays to give an air of authenticity to their messages. Or they take advantage of news events and crises like natural disasters to trick you into clicking to donate to a scam charity. Another common scenario involves shipping and delivery services where scammers may request personal information in order to complete a delivery.

You can find the NIST Phishing video and other SBCC videos at: https://www.nist.gov/itl/smallbusinesscyber/videos

Can you spot a phishing attack sometimes you can avoid trouble by just deleting the message. Some of the signs might include:

1. Suspicious looking source email address
2. Generic greeting like "Dear customer" – instead of the customization most organizations offer
3. Spoofed hyperlinks -- if you can hover your mouse over the link, the destination displayed in the preview might be completely different than the destination displayed in the message

4. Poor spelling, or sloppy layout
5. Suspicious or unusual attachments – treat all attachments and links with caution

How to avoid being tricked by phishing

1. Always be suspicious of any message that requests you to click a link or open an attachment.
2. Be cautious of any message communicating a sense of urgency or dire consequences should you fail to take immediate action.
3. If you are concerned about a message, contact the person or the organization using a different, validated method like a phone number you already had or check the organization's website 'Contact Us' information. Never use the links or contact information in the message you are concerned about.
4. Be careful not to provide personal or sensitive information in response to a message.

What can your small business do?

- Deploy and maintain anti-virus software – if the phishing attack aims to install malware on your computer, up-to-date anti-virus software may help prevent the malware from installing.
- Utilize email filters – many email services have configurable filters which can help prevent many phishing messages from ever reaching users' mailboxes.
- Configure email security technologies –email services can also implement email authentication technologies that verify where messages originated and can reject messages that are spoofed. Check with your provider to see what security options are available.
- Enable anti-phishing capabilities – email clients and web browsers often have anti-phishing capabilities. Enable available capabilities to help protect against phishing attacks.
- Implement multi-factor authentication (MFA) – MFA requires an additional forms of authentication (e.g., a code texted to your phone number) in addition to your password. If MFA is enabled for your accounts, an attacker may still not be able to access your account even if you are tricked into providing your password.

What should you do if a phishing attack is successful?

- Change any affected passwords – If possible, immediately change the password for any affected accounts. If this password was also used for other online accounts, change the passwords for those accounts to something unique and strong.
- Contact the fraud department of the breached account – If the phishing attack compromised your company's account at a financial institution, contact the bank immediately to report the incident. Monitor for unauthorized transactions to the account. If a personal account was involved, contact the 3 major credit bureaus to enable fraud alerts.
- Notify appropriate people in your company – follow your company's incident response plan to ensure the appropriate personnel are aware of the incident.
- Notify affected parties – if personal data of others (e.g., customers, suppliers) was compromised, be sure to notify them. The compromised personal data could be used for identity theft. Check the website of your state's attorney general for information on data breach notification requirements.