NIST Small Business Cybersecurity Fact Sheet

Phishing

What is Phishing?

Phishing is the use of convincing emails or other messages to trick us into opening harmful links or downloading malicious software. These messages are often disguised as a trusted source, such as your bank, credit card company, or even a leader within your own business.

How to Spot a Phish

Artificial intelligence (AI) can now be used to craft increasingly convincing phishing attacks, so it is more imperative than ever to take a second, or third, look at any message requesting you to take action—such asking you to click a link, download a file, transfer funds, log into an account, or submit sensitive information. What to look out for:

- A request to download an attachment or click on a link– treat all attachments and links with caution.
- A sense of urgency. They want you to act now. Stop and take a moment to think about the request. Verify the request by using known contact information or information from a public company website, not from the message itself. Or if you get an urgent message from your boss or a vendor, contact them directly to verify the message.
- Suspicious looking source email address. Would your bank email from Chase@***gmail.com***?
- A request for sensitive information, like bank account information or Social Security number.

How Can I Protect My Business From Phishing?

- Teach employees how to spot and report a phish when they have fallen victim or think they have fallen victim to a phishing attack.
- Recognize that email isn't the only way to get phished. You can also receive attacks through text messages, phone calls, social media messages, or even physical postal mail.
- Don't engage with the sender, and do not click any link in the email (including unsubscribe). Just delete the message. You can report phishing crimes to the FBI's Internet Crime Complaint Center.
- 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 that can help prevent many phishing messages from ever reaching your employees' 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 multi-factor authentication. Take it to the next level by implementing phishing-resistant authentication. Learn more here.

NIST Small Business Cybersecurity Fact Sheet

Phishing

What should I do if I think I've been a victim of a phishing attack?

- **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.

Questions to Consider

- Do our employees know how to spot a phish?
- Are we regularly training employees to raise their awareness of phishing threats?
- Do our employees know how to report if they think they have fallen victim to a phishing attack?
- Is multi-factor authentication (MFA) required and used on all accounts that offer it? Especially accounts that access sensitive information? Are we using phishing-resistant MFA?
- Are we regularly updating our business technologies and software when updates are available?

Related Resources

- NIST Human-Centered Cybersecurity Phishing Resources: https://csrc.nist.gov/projects/human-centered-cybersecurity/research-areas/phishing
- Recognize and Report Phishing (Cybersecurity and Infrastructure Security Agency) https://www.cisa.gov/secure-our-world/recognize-and-report-phishing