Food Safety and Inspection Service
U.S. DEPARTMENT OF AGRICULTURE

Food Defense – Cyber Security
Phishing

You receive an email that looks like it is from someone you know and appears to be from a shipping company you use which asks that you click on a link to learn about a shipping delay. Should you click on the link? Probably not. This may be a phishing attempt.

What is Phishing?

Phishing is a form of social engineering that utilizes email or malicious websites to solicit personal information or tricks you into downloading malicious software by posing as a trustworthy entity.

How Phishing Works

- You get an email or text that seems to be from someone you know which asks you to click on a link or requests that you provide a password, bank account number, or other sensitive information.
- It looks real. Scammers often spoof logos and make up fake email addresses.
- It's urgent. Messages often pressure you to act now or something bad will happen.
- What happens next? If you click on a link, you grant scammers an opportunity to install ransomware or other programs that can restrict data access and may spread through the entire company network. Sharing password information allows scammers access to accounts.

Preventing Phishing

Before you click on a link or share any sensitive business information, look for:

- Suspicious sender's address that may imitate a legitimate business.
- Generic greetings and signature and a lack of contact information in the signature block.
- Spoofed hyperlinks and websites that do not match the text when hovering over them.
- Misspelling, poor grammar or sentence structure, and inconsistent formatting.
- Suspicious attachments or requests to download and open an attachment.
- A website or phone number for the company or person behind the text or email to make sure you are being contacted by a legitimate business.
- The name of the company and call to confirm that they need the requested information from you. Use a phone number that you know is correct, not the one provided in the email or text message.

Protecting Your Business

- Back up your data on a regular basis and make sure those backups are not connected to the network.
- Keep all security up to date. Always install the latest patches and updates.
- Alert your staff if you receive information about new phishing threats.
- Deploy a safety net. Use email authentication technology to help prevent phishing emails from reaching your company's inboxes.

Responding to a Phishing Scheme

Even though the recommended protective measures may be in place, a member of your organization may still be fooled by a phishing scheme. Take the following steps if you or a member of your organization falls prey:

- Alert others. Talk to your colleagues and share your experience. Phishing attacks often happen to more than one person in a company.
- Limit the damage. Immediately change any compromised passwords and disconnect from the network any computer or device that is infected with malware.
- Follow your established procedures, including notifying specific people in your organization or contractors that provide IT support.
- Notify your customers if your data or personal information has been compromised. They could be at risk of identity theft. You can find information on how to do so by accessing this resource: A Guide for Business | Federal Trade Commission (ftc.gov).
- Report it. Forward phishing emails to reportphishing@apwg.org. Let the company or person that was impersonated know about the phishing scheme, and report it to the Federal Trade Commission at reportfraud.ftc.gov/#1.

Helpful Links

- Cybersecurity & Infrastructure Security Agency (CISA) Cyber Hygiene Services
- NIST Small Business Cyber Security Corner
- CISA Phishing Postcard
- Federal Trade Commission Cyber Security for Small Business
- CISA Regional Cyber Security Advisors