SAFE Tip Sheet

Phishing - YOU are a Target!

Phishing is a leading cause of data breaches, and it only takes one click to compromise your network. Some departments are more frequently targeted because they receive a high volume of emails, give employee support, or have access to executives and/or confidential information. However, employees in all areas are targets for company spear-phishing campaigns, so make sure you take steps to protect yourself and your company.

Phishing emails often impersonate an executive, the help desk, IT, or a well-known company you work with or would know. They may appeal to your job duties or urgently need you to send some information, click on a link, or download an attachment.

Common Phishing themes include:

- Request from an executive (urgent)
- Request to sign a document (DocuSign)
- Overdue payment
- Password check/change required
- Dropbox: Document Shared with You
- Update or verify account information
- Resume or job offer
- Follow Up
- Problems with your account

What to watch for:

- Generic greetings (i.e., "Dear customer")
- Misspellings or bad grammar
- Return email address does not match Sender*
- Deceptive links (hover over them to verify the actual address)
- Some urgent need for... (fill in the blank!)

Phishing for Credentials

Attackers want your login information for email accounts, internal networks, and banking accounts. Phishing emails can fool you by using copies of logos, signatures, and brand colors - but when you click on the link, it takes you to a fraudulent login page (although these can look quite convincing) that will capture your username and password. Be sure to hover over the link to see where it's going. Or better yet, use a known link to the actual site.

Remember...

- **Be skeptical of urgent requests** that don't follow typical company procedures you would expect or normal behavior.
- **Don't interact with unsolicited links and attachments.** Unsolicited links or files, even from a sender you recognize, can be used to distribute malware.
- **Set up multi-factor authentication (MFA).** Strengthen the security of your accounts by setting up MFA whenever it is offered.
- **Always verify** that the email is legitimate with a quick phone call if it seems unusual or requests personal or company-sensitive information.

If you suspect that you have received a spear-phishing email at work, follow your procedures for reporting it immediately.

**Note: Mailing services (i.e., Mailchimp) can change the Sender in an email to show which company is sending the email.*