Delivering IT Peace Of Mind

ANP ADVANCED NETWORK PRODUCTS

33 East Glenside Avenue, Glenside, PA 19038-4601
215-572-0111 Fax: 215-885-9933 www.anp.net

Examples of Phishing Messages

You open an email or text, and see a message like these:

"We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."

"During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."

“Our records indicate that your account was overcharged. You must call us within 7 days to receive your refund.”

The senders are phishing for your information so they can use it to commit fraud.

How to Deal with Phishing Scams

- *Delete email and text messages that ask you to confirm or provide personal information (credit card and bank account numbers, Social Security numbers, passwords, etc.). Legitimate companies don't ask for this information via email or text.*
- *The messages may appear to be from organizations you do business with – banks, for example. They might threaten to close your account or take other action if you don’t respond.*
- *Messages may also appear to come from internal addresses.*
- *Don’t reply, and don’t click on links or call phone numbers provided in the message, either. These messages direct you to spoof sites – sites that look real but whose purpose is to steal your information so a scammer can run up bills or commit crimes in your name.*
- *Area codes can mislead, too. Some scammers ask you to call a phone number to update your account or access a "refund." But a local area code doesn’t guarantee that the caller is local.*
- *If you’re concerned about your account or need to reach an organization you do business with, call the number on your financial statements or on the back of your credit card.*

10 Tips to Prevent Phishing Attacks

1. Learn to Identify Suspected Phishing Emails

- Below are some characteristics that identify an attack through an email:

They duplicate the image of a real company.
Copy the name of a company or an actual employee of the company, including your organization.
Include sites that are visually similar to a real business.
Promote gifts, the loss of an existing account, even request a specific piece of information not typically expected.

2. Check the Source of Information from Incoming Mail

- *Financial institutions will never ask you to send your passwords or personal information by mail. Never respond to these questions, and if you have the slightest doubt, call your bank directly for clarification.*

3. Never go to a financial institution's website by clicking on links included in emails

- *Do not click on hyperlinks or links attached in the email, as it might direct you to a fraudulent website.*
- *Type in the URL directly into your browser or use bookmarks / favorites if you want to go faster.*

4. Enter Your Sensitive Data in Secure Websites Only

- *In order for a site to be 'safe', it must begin with 'https://' and your browser should show an icon of a closed lock.*

5. Phishing Doesn't Only Pertain to Online Banking

- *Most phishing attacks are against banks, but can also use any popular website to steal personal data such as eBay, Facebook, PayPal, etc.*

6. Phishing Knows All Languages

- *Phishing knows no boundaries, and can reach you in any language. In general, they're poorly written or translated, so this may be another indicator that something is wrong.*

7. Have the Slightest Doubt, Do Not Risk It

- *The best way to prevent phishing is to consistently reject any email or news that asks you to provide confidential data.*
- *Submit a ticket to the ANP team to investigate your concern. Better safe then sorry.*