E-Report Phish Training Modules

What Is A Phishing Email?

A Phishing email when someone tries to trick you into sharing personal and / or financial information online.

Phishing scams are designed to trick people in handing over usernames and passwords, which can be used to access protected data, networks and systems.

Phishing attacks are becoming increasingly sophisticated, with many fake emails being almost entirely indistinguishable from real ones.

https://www.kashflow.com/handle-phishing-attack/
https://support.google.com/mail/answer/8253?hl=en

What Does Common Phishing Emails Look Like?

Phishing is usually done through email. For example, someone who is phishing might send you an email that looks like it's from your bank so that you'll give them information about your bank account.

Key Signs Of A Phishing Email

Phishing emails or sites might ask for:

- Usernames and passwords, including password changes
- Social Security numbers
- Bank account numbers
- PINs (Personal Identification Numbers)
- Credit card numbers
- Your mother’s maiden name
- Your birthday

https://support.google.com/mail/answer/8253?hl=en

What Are The Various Phishing Attack Techniques

- Embedding a link in an email that redirects your employee to an unsecure website that requests sensitive information
- Installing a Trojan via a malicious email attachment or ad which will allow the intruder to exploit loopholes and obtain sensitive information
- Spoofing the sender address in an email to appear as a reputable source and request sensitive information
- Attempting to obtain company information over the phone by impersonating a known company vendor or IT department

https://digitalguardian.com/blog/phishing-attack-prevention-how-identify-avoid-phishing-scams

How To Avoid Receiving Phishing Emails

Your email spam filters may keep many phishing emails out of your inbox. But scammers are always trying to outsmart spam filters, so it’s a good idea to add extra layers of protection. Here are four steps you can take today to protect yourself from phishing attacks.

How To Help Protect Yourself From Phishing Emails

1. Protect your computer by using security software. Set the software to update automatically can deal with any new security threats.

2. Protect your mobile phone by setting software to update automatically. These updates could give you critical protection against security threats.

3. Protect your accounts by using multi-factor authentication. Some accounts offer extra security by requiring two or more credentials to log in to your account. This is called multi-factor authentication. The additional credentials you need to log in to your account fall into two categories: Something you have — like a passcode you get via text message or an authentication app. Something you are — like a scan of your fingerprint, your retina, or your face. Multi-factor authentication makes it harder for scammers to log in to your accounts if they do get your username and password.

4. Protect your data by backing it up. Back up your data and make sure those backups aren’t connected to your home network. You can copy your computer files to an external hard drive or cloud storage. Back up the data on your phone, too.

https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

How To Handle A Phishing Email

If an email looks suspicious, don't risk your personal information by opening or responding to the message. Below are some suggested guidelines to help protect yourself against these threats when suspicious mail arrives within your mailbox:

1. If you receive a phishing e-mail message, do not respond to it. Don't open junk mail at all
2. Approach links in email messages with caution
3. Approach images in e-mail with caution
4. Approach attachments in email messages with caution
5. Don't trust the sender information in an e-mail message
6. Don't trust offers that seem too good to be true
7. Report suspicious email

What To Do If You Have Responded To The Email

If you think a scammer has your information, like your Social Security, credit card, or bank account number, go to IdentityTheft.gov. There you'll see the specific steps to take based on the information that you lost.

If you think you clicked on a link or opened an attachment that downloaded harmful software, update your computer's security software. Then run a scan.

https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams
https://www.identitytheft.gov/Info-Lost-or-Stolen

How To Report Phishing Emails

If the email came from a gmail client do the following or use report link:

On a computer, go to Gmail. -->Open the message. -->Next to Reply Reply, click More More. Note: If you're using classic Gmail, click the Down arrow Down Arrow. Click Report phishing.

https://support.google.com/mail/contact/abuse

If you got a phishing email or text message, report it. The information you give can help fight the scammers.

Step 1. If you got a phishing email, forward it to the Anti-Phishing Working Group at reportphishing@apwg.org. If you got a phishing text message, forward it to SPAM (7726).

Step 2. Report the phishing attack to the FTC at ftc.gov/complaint.

You can also report it to the College by forwarding the email is the following address: phishing@plattsburgh.edu

https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

Sources