Protect yourself from phishing

Phishing (pronounced: fishing) is an attack that attempts to steal your money, or your identity, by getting you to reveal personal information -- on websites that pretend to be legitimate. Cybercriminals or scam artists send official-looking emails, attempting to fool you into disclosing your personal information — such as user names, passwords, banking records or account numbers, or social security numbers — by replying to the email or entering it on a phone website.
Phishers can pretend to be from a legitimate bank, organization, government agency, or store, or claim to be the host of a lottery or contest.

PHISHING EMAILS

Phishing is a popular form of cybercrime because of how effective it is. The best defense is awareness and knowing what to look for.

Here are some ways to recognize a phishing email:

- **Urgent call to action or threats** - Be suspicious of emails that claim you must click, call, or open an attachment immediately. Often, they'll claim you have to act now to claim a reward or avoid a penalty. Creating a false sense of urgency is a common trick of phishing attacks and scams. They do that so that you won't think about it too much or consult with a trusted advisor who may warn you.

  Tip: Whenever you see a message calling for immediate action take a moment, pause, and look carefully at the message. Are you sure it's real? Slow down and be safe.

- **First time or infrequent senders** - While it's not unusual to receive an email from someone for the first time, especially if they are outside your organization, this can be a sign of phishing. When you get an email from somebody you don't recognize, or that Outlook identifies as a new sender, take a moment to examine it extra carefully before you proceed.
- **Spelling and bad grammar** - Professional companies and organizations usually have an editorial staff to ensure customers get high-quality, professional content. If an email message has obvious spelling or grammatical errors, it might be a scam. These errors are sometimes the result of awkward translation from a foreign language, and sometimes they're deliberate in an attempt to evade filters that try to block these attacks.
- **Generic greetings** - An organization that works with you should know your name and these days it's easy to personalize an email. If the email starts with a generic "Dear sir or madam" that's a warning sign that it might not really be your bank or shopping site.

- **Mismatched email domains** - If the email claims to be from a reputable company, like Microsoft or your bank, but the email is being sent from another email domain like Gmail.com, or microsoftsupport.ru it's probably a scam. Also be watchful for very subtle misspellings of the legitimate domain name. Like micros0ft.com where the second "o" has been replaced by a 0, or rnicrosoft.com, where the "m" has been replaced by an "r" and a "n". These are common tricks of scammers.
- **Suspicious links or unexpected attachments** - If you suspect that an email message is a scam, don't open any links or attachments that you see. Instead, hover your mouse over, but don't click, the link to see if the address matches the link that was typed in the message. In the following example, resting the mouse over the link reveals the real web address in the box with the yellow background. Note that the string of numbers looks nothing like the company's web address.

Tip: On Android long-press the link to get a properties page that will reveal the true destination of the link. On iOS do what Apple calls a "Light, long-press".

Cybercriminals can also tempt you to visit fake websites with other methods, such as text messages or phone calls. Sophisticated cybercriminals set up call centers to automatically dial or text numbers for potential targets. These messages will often include prompts to get you to enter a PIN number or some other type of personal information.

AWARENESS ON MALICIOUS E-MAILS?

1. Identify the Sender. Do you know this person? Were you expecting e-mail from this person or does it fit in with your job role? If not, it is probably suspicious.
2. Reply-to. If the Reply-to address is different from the sending address, this should raise your suspicion for the whole message.
3. Links and Attachments. If you were not expecting an attachment or a link, and you do not know the sender, do not open it! If you are not sure, check with the sender by phone (don’t use a phone number in the e-mail), otherwise report it.
4. Grammar and Tone. Many of the malicious e-mails sent have poor grammar, punctuation and spelling. In addition, you should know how your co-workers communicate. Does this message sound like them? If not, it is probably malicious.
5. Emotions. Be wary of any e-mails trying to cause certain emotions. The most commonly-used malicious emotions are:
    a. Greed. Messages offering or promising you money by clicking a link or giving away information are usually.malicious. If it seems too good to be true, it probably is.

b. Urgency. Unusually short deadlines create a false sense of urgency to act. Attackers employ this technique inattempts to confuse the recipient.
c. Curiosity. Attackers take advantage of our curiosity by promising something exciting or prohibited content.
d. Fear. Threatening recipients with negative consequences is a common tactic to generate responses—things suchas threatening to shut off accounts or legal action.

TIPS TO AVOID A PHISHING SCAM

1. **Be on the lookout for suspicious emails or text messages**. Legitimate, responsible companies will never solicit personal information over email. Never reveal personal or financial information in response to an email request, no matter who appears to have sent it.
2. **Don't click on links or attachments in suspicious emails or text messages**. If you receive a suspicious message from an organization and worry the message could be legitimate, go to your web browser and open a new tab. Then go to the organization's website from your own saved favorite, or via a web search. Or call the organization using a phone number listed on the back of a membership card, printed on a bill or statement, or that you find on the organization's official website.
3. **Set up a spam filter.** A spam filter can greatly reduce the number of phishing emails you receive. University IT provides free spam management for University email.
4. **If you are still tempted to click, pick up the phone instead.** If the message looks real and you are really tempted to respond, instead look up the phone number of the company and call them. Do not use any phone number in the email because it could be fake. Ask if the message was actually sent by the company and if you can take care of any issues over the phone instead.
5. **Change your passwords regularly.** Whether or not you've fallen victim to a suspicious email, it is best to practice safe security by changing your password on a regular basis. Unlike keys or an ATM card, your password does not have to be physically taken to be copied, and it's unlikely you'll know when your password has been stolen. Visit University IT's passwords page for tips to creating a strong password.
6. **From a person you know:** If the suspicious message appears to come from a person you know, contact that person via some other means such as text message or phone call to confirm it.

What to do if you think you've been successfully phished

If you're suspicious that you may have inadvertently fallen for a phishing attack there are a few things you should do.

1. While it's fresh in your mind write down as many details of the attack as you can recall. In particular try to note any information such as usernames, account numbers, or passwords you may have shared.
2. Immediately change the passwords on those affected accounts, and anywhere else that you might use the same password. While you're changing passwords you should create unique passwords for each account.
3. Confirm that you have multifactor authentication (also known as two-step verification) turned on for every account you can.
4. If this attack affects your work or school accounts you should notify the IT support folks at your work or school of the possible attack. If you shared information about your credit cards or bank accounts you may want to contact those companies as well to alert them to possible fraud.
5. If you've lost money, or been the victim of identity theft, report it to local law enforcement. The details in step 1 will be very helpful to them.

HOW CAN I MAKE SURE MY MESSAGE LOOKS LEGITIMATE?

Several actions will help make your messages look legitimate.

1. Use links to sites with “https://” This directs your recipients to websites that can be verified by a trusted third party.
2. Offer alternatives to clicking the link. Give directions such as “Go to the Intranet, click on …”
3. Have direct contact information. Give your recipients a point of contact to verify the authenticity of the message.
4. Avoid attachments. Where possible avoid sending attachments. Try to use departmental file shares or other methods of file transfer.