



Attention all Employees:

With the latest ransomware virus spreading around the world and recent phishing attempts, I wanted to take this opportunity to refresh everyone's memories on practicing safe web browsing and email use.

**Please read the following carefully and save for future reference.** One careless click can be devastating to yourself and the entire company.

General Guidelines:

1. **NEVER click on an email link or attachment unless you're 100% sure where the link leads or what the attachment is, even if the email seems like it is coming from a known source.** Phishing often works by deceitfully using a name or email address from someone in your contacts. It is also possible that the sender's PC was compromised by a virus that is sending emails to everyone in their address book.
2. **Type in the website manually in another tab if you are unsure about the authenticity of a link.** Many phishing emails will pose as trusted companies and prompt you to follow in link in order to validate your email or other information. Instead of following the link they provide, go to the website yourself and check if it truly needs you to validate something.
3. **Be on the lookout for irregularly worded or formatted emails.** If the subject line or the body of the email seems unusually vague or incomplete, **DO NOT OPEN THE ATTACHMENT OR CLICK ON LINKS**, even if you recognize the sender. Double check with the sender through alternate means to ensure authenticity.
4. **Don't press CANCEL on pop-up window, always close the window by pressing X on the top right corner.** Any button on the window itself, including buttons like "cancel," may actually be a disguised link that will download a virus.
5. **Don't blindly follow instructions from a pop-up.** Many malicious pop-ups will pose as, or being affiliated with, trustworthy companies and instruct you to either call a certain number or go to a certain website. Always manually search for the phone number or

website rather than risking getting scammed.

6. **Always confirm that the URL of a website matches the domain name of the organization.** A quick look at your browser's web address bar to ensure that it's the same as the organization name and web address is an easy way to spot malicious sites.
7. **If you think an offer is too good to be true, it probably is.** Be vigilant and do proper research before accepting an offer. Enticing deals are a common way scammers can get your information.

### Email Attachments and Viruses

One of the most common way computer viruses and worms spread is through email attachments. If these attachments are opened, they can give hackers **complete control of your machine and initiate attack on other machines**. They can also start sending out copies of itself to any email address it finds in your contacts under your name. Malicious software (malware) like this has crippled personal machines, email servers, businesses, government networks, and countless other organizations.

Just because you may consider yourself tech-savvy doesn't mean you can be careless. Scammers are always finding new, sneaky ways to attack.

Here are a few guidelines that will help you stay safe from malicious attachments:

1. **Don't open attachments if the email looks strange**, even if the message is from a user you regularly exchange emails with. Things to look out for are vague or incomplete subject lines or message body, several unexpected messages from different people with identical subject lines, or any other irregularity.
2. **Don't open unusual attachments.** Most attachments you receive probably fall into a few recognizable categories: Word (.doc), Excel (.xls/.xlsx), PowerPoint (.ppt), PDFs, and the like. Attachments with unusual icons or extensions (like .pif, .scr, or .exe) should not be opened without first thoroughly verifying its safety.
3. **Don't open unexpected attachments and/or attachments from strangers.** Generally, if a malicious attachment is not opened or viewed, it cannot infect your computer. If you know the person who send the email, but weren't expecting them to send you an attachment, contact them and confirm that they sent it before opening.

## Phishing Scams

A phishing scam is an email where the perpetrator sends a legitimate looking email that usually appear to come from a well-known and trustworthy organization or website in an attempt to gather personal and financial information from the recipient.

There are two common types of phishing scams:

- A. **An email containing an urgent request for personal information.** You'll be asked to respond to an email with account information, DOB, SSN, and the like in order to prevent immediate closure of your account. These emails can even be personalized.
- B. **An email containing a link and a request to verify your account.** Even if the link appears to take you to a valid website, it may be a counterfeit website designed especially to mimic the real one and seize your information. Unless you are expecting a verification email (i.e. you requested to change your password or username), never click on the link even if it seems legitimate.

ANY EMAIL ASKING YOU TO DIRECTLY RESPOND WITH SENSITIVE INFORMATION OR ASKING UNPROMPTED TO VALIDATE CERTAIN INFORMATION ARE ALMOST ALWAYS PHISHING ATTEMPTS.

An easy solution is to open another tab, go to the website the email is claiming to be sent from, and check your account that way. If there actually is a problem with your account, you will be able to take care of it safely. If everything looks fine, then congratulations! You just successfully avoided getting phished.