How to Recognize Phishing/Spam Email

Scammers use email or text messages to trick you into giving them your personal information. They may try to steal your passwords, account numbers, or Social Security numbers. If they get that information, they could gain access to your email, bank, or other accounts. Scammers launch thousands of phishing attacks like these every day — and they're often successful. The FBI's Internet Crime Complaint Center reported that people lost $57 million to phishing schemes in one year.
Scammers often update their tactics, but there are some signs that will help you recognize a phishing email or text message.

Phishing emails and text messages may look like they are from a company you know or trust. They may look like they are from a bank, a credit card company, a social networking site, an online payment website or app, or an online store.
Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment. They may

- say they've noticed some suspicious activity or log-in attempts.
- claim there's a problem with your account or your payment information.
- say you must confirm some personal information.
- include a fake invoice
- want you to click on a link to make a payment.
- say you're eligible to register for a government refund.
- offer a coupon for free stuff.

Here's a real world example of a phishing email.

Imagine you saw this in your inbox. **Do you see any signs that it's a scam?** Let's take a look.

- The email looks like it's from a company you may know and trust: Netflix. It even uses a Netflix logo and header.
- The email says your account is on hold because of a billing problem.
- The email has a generic greeting, "Hi Dear." If you have an account with the business, it probably wouldn't use a generic greeting like this.
- The email invites you to click on a link to update your payment details.

While, at a glance, this email might look real, it's not. The scammers who send emails like this one do not have anything to do with the companies they pretend to be. Phishing emails can have real consequences for people who give scammers their information. And they can harm the reputation of the companies they're spoofing.

What to Do If You Suspect a Phishing Attack?

If you get an email or a text message that asks you to click on a link or open an attachment, answer this question:
Do I have an account with the company or know the person that contacted me?
If the answer is "No," it could be a phishing scam. Go back and review the tips in How to recognize phishing and look for signs of a phishing scam. If you see them, report the message, and then delete it.

If you determine that this email is Phishing/Spam, Microsoft has a built-in learning system that will learn as you categorize. Please right click the email, go to Junk, and block sender. Anytime you receive an email that looks suspicious or you do not recognize the sender this will be your best practice.

As Microsoft learns this will assist in preventing future spam emails.

If the answer is "Yes," contact the company using a phone number or website you know is real. Not the information in the email. Attachments and links can install harmful malware.
If you have reviewed the above and still have questions, contact Stringfellow Technology Group support desk for further direction.