Phishing and Smishing (SMS Phishing)

Phishing is an attack that attempts to steal your money, or your identity, by getting you to reveal personal information -- such as credit card numbers, bank information, or passwords -- on websites that pretend to be legitimate. Cybercriminals typically pretend to be reputable companies, friends, or acquaintances in a fake message, which contains a link to a phishing website. Cybercriminals have also been successful using emails, text messages, and direct messages on social media or in video games, to get people to respond with their personal information. The best defence is awareness and knowing what to look for.

Here are some ways to recognise a phishing email:

- **Urgent call to action or threats** - Be suspicious of emails and text messages 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, infrequent senders, or senders marked [External]** - While it's not unusual to receive an email or text message from someone for the first time, this can be a sign of phishing. Slow down and take extra care at these times. When you get an email or a text message from somebody you don't recognise, or that Outlook identifies as a new sender, take a moment to examine it *extra* carefully using some of the measures below.

- **Spelling and bad grammar** - Professional companies and organizations usually have an editorial and writing staff to make sure 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, or a text 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. Look at the address that pops up when you hover over the link. Ask yourself if that 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. The string of numbers looks *nothing like* the company's web address.

Cybercriminals can also tempt you to visit fake websites with other methods, such as text messages or phone calls. If you're feeling threatened or being pressured, it may be time to hang up, find the phone number of the establishment and call back when your head is clear. Sophisticated cybercriminals set up call centres 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.