# PROTECT YOURSELF FROM ONLINE SCAMS AND ATTACKS

One of the most common attacks we see are what we call “phishing” attacks (pronounced like fishing). This is when an attacker contacts you pretending to be somebody you know or an organization you trust, and tries to get you to give them personal information or open a malicious website or file.

Most phishing attempts arrive via email, but they can also come via text messages, direct messages on social media, or even phone calls. What they all have in common are:

## A trusted sender

The message or call will appear to come from a person or organization you trust. Could be your bank, the government, a service like Cox, Netflix or Spotify, a tech company like Microsoft, Amazon, or Apple, or some other service you recognize.

## An urgent request

The messages usually have a sense of urgency to them. Something is going to be canceled, you’re going to have to pay some kind of penalty, or you’re going to miss out on some kind of special deal, and you have to act NOW.

The urgency is to get you to take the message seriously and also to get you to act on the message without thinking about it too much, consulting a trusted advisor, or looking into whether the message might be a fake.

## A link or attachment

The message will include something you need to click on – a link to a website, or an attached file most commonly. The website will likely be a fake version of a legitimate website, designed to fool you into entering your username and password, or other personal information, so they can steal that information to use themselves. Any attached file is almost certainly malware.

## What can you do about phishing?

Look carefully at any messages you get that want you to take urgent action. Pay particular attention to the email address of the sender. If the message claims to be from your bank but the sender’s address is not your bank’s domain name that should be a loud warning.

Never open any links or attachments you weren't expecting; even if they appear to come from somebody you trust.

If you get a link that appears to be from your bank or other trusted organization, open a new tab in your web browser and go directly to the organization's website from your own saved favorite, from a web search, or by typing in the organization's domain name yourself. A link from a phishing email will take you to a site that looks very genuine but is designed to trick you into entering your personal information.

If you get an attachment you weren't expecting, don't open it. Instead reach out to the sender, preferably via a different method like text message or phone call, and confirm that the attachment is genuine before you open it.

Finally, use **SmartScreen for Microsoft Edge** which can help to block known phishing websites.

**SmartScreen** is a security feature in **Microsoft Edge** that helps protect you from phishing and malware sites and software, and helps you make informed decisions about downloads. It checks the sites you visit against a dynamic list of reported phishing and malicious software sites and warns you if the site has been blocked for your safety. It also checks your downloads against a list of reported malicious software sites and programs known to be unsafe, and warns you if the download has been blocked for your safety.

SmartScreen also analyzes web pages as you browse the web and determines if they might be suspicious. If it finds a suspicious site, SmartScreen displays a warning page advising you to continue with caution and giving you an opportunity to provide feedback to Microsoft.

You can turn SmartScreen on or off in Microsoft Edge by selecting **Settings and more > Settings > Privacy, search, and services > Security**, and then turning Microsoft Defender SmartScreen on or off.