How to Fight Phishing

AVAST CYBERHOOD WATCH **TOOLKIT**

How to Fight Phishing?

Phishing is the malicious use of email and SMS to send fraudulent messages to unsuspecting victims. Phishing attacks are designed to trick people into giving up personal information, such as passwords and credit card numbers, or downloading malware to their devices that could be used to eavesdrop or lock computers and files until a ransom is paid. Here are four top tips that will help you avoid falling victim.

1. **Double check the links.** Many phishing emails include links to malicious sites that look like the real deal and are hard to recognise as fake. Today's cybercriminals are using new technologies to personalise emails with information that people share about themselves online. If you receive an email that looks suspicious, don't click on any links or open attachments in the message. Instead, copy and paste the links directly into the address bar of your browser (e.g. Google Chrome, Mozilla Firefox).

2. **Double check the content and context.** Are there grammatical and punctuation errors? Is the writing style dissimilar to previous messages from the "same" sender (e.g. your bank)? Is there an over dramatic sense of urgency in the message? These characteristics may indicate that the message is malicious.

3. **Check for the padlock.** When you open a browser and visit a website, keep an eye out for the padlock icon on the left-hand side of the browser address bar. This icon indicates that any data you send over the web is protected. If a page does not have the padlock or it's crossed out, refrain from entering any personal data and financial information on the site.

4. **Install a strong antivirus.** Always make sure your devices and your applications are up-to-date and install a strong antivirus with an anti-phishing feature to prevent the bad guys from stealing your personal information.