

## What is Phishing? Transcript

What is Phishing?

Phishing is a cybercrime in which an attacker tries to gain valuable information, by disguising communications as being from a reputable source.

Who would fall for that?

Cyber criminals can be very good at impersonating people or organisations that you trust. They aim to fool you into handing over valuable information such as passwords, PIN numbers and account numbers. Cyber criminals usually launch phishing attacks by email, instant messaging services or other communication channels.

Why do they use Phishing?

Phishing is a very popular tool for cyber criminals. It allows them to target thousands of potential victims at a time. It is easier for a hacker to trick an individual into clicking on a malicious link, than to break through an organisation's digital defences.

How does it work?

Once an individual falls for a phishing scam, usually by clicking on a fraudulent link, hackers will install malicious software or steal personal information from their computer.

What should I do?

Best practice for avoiding these scams is to increase your awareness.

Always be alert for tell-tale signs of phishing, including lucrative offers designed to catch your eye, usually from suspicious senders.

Communications with a sense of urgency that ask you to act now, or emails containing links which may not appear to be as they seem, may also be warning signs of a phishing attack.

Always remember that emails sent by colleagues, friends and family should be treated with caution, especially if you are not expecting an email from them or if their email contains unexpected attachments. These emails could be coming from a hacked account.