# THE SOCIAL ENGINEERING GLOSSARY

PDSC
POLICE DIGITAL SECURITY CENTRE

## Baiting

Luring the victim with something appealing, encouraging them to act in response, compromising their security in doing so. The enticement is not always in the cyber world, in the real world there may be an infected USB lying on the ground that you may plug into your device. Never connect rogue equipment to your network. If it is too good to be true, it usually is.

## Pretexting

Building trust before deploying the attack. An adversary will make up a convincing backstory that connects with you, not necessarily asking for anything initially. Once your guard is down, they will make their request and based on what you know you would most likely be obliging. No matter the story, never disclose information or send money in response.

## Pharming

Redirecting visitors from a legitimate website, to a malicious copycat site. This is achieved with the use of malicious code either on a DNS server or your device. You might have been visiting the site to login or complete a form but you would be disclosing information to the hacker. Use Quad9 to block known malicious sites and look for https in web addresses.

## Phishing

Fraudulent scams via email. Often an adversary would send generic emails to many people in the hope someone would fall for it. Take precautions if the email is not addressed personally.

## Quid Pro Quo

The act of doing something in return for something. In the context of a scam, a criminal could phone up and pretend to be tech support. The victim could coincidentally need help, disclosing information or even allowing remote access to the device. If tech support calls you up, asking for information or access to your device, hang up and call them on a number you know.

## Scareware

Pop-ups that scare the victim into clicking, for instance masquerading as antivirus that has found malicious content on the system. They are then redirected to a website where they are tricked into buying unnecessary and possibly dangerous products. Do not click on any pop-ups that appear and use reputable sites to purchase new software.

## SMiShing

Fraudulent scams via text, similarly to phishing. Phone numbers can often be spoofed to look genuine. An adversary may pretend to be someone you know and seek a reply. Do not reply to these messages as you could be charged. If in doubt use the contact information you have for the individual.

## Spear Phishing

Fraudulent emails that are targeted towards an individual or business. Information about the victim can be obtained from platforms such as social media, to make the scam more convincing. Verify the email address it was sent from and look out for minor spelling differences such as the subtle change of an o to 0.

## Tailgating

An unauthorised individual gains access to restricted premises by following closely behind an authorised individual, perhaps claiming to have forgotten a pass or unable to swipe because their hands are full. Be vigilant on any suspicious activity. Challenge people you do not recognise.

## Vishing

Fraudulent scams via phone call. Phone numbers can often be spoofed to look genuine (possibly to appear from the bank) so be wary of what the caller is asking. Put the phone down and call back on a legitimate phone number.

## Watering Hole

Scams are aimed at specific groups such as an organisation, government, industry, etc. Criminals will gain access to the systems by infecting the websites most frequented by the target group. It is difficult to detect this attack so *do not* browse the internet on work equipment unless absolutely necessary for the job role.

## Whaling

When the target is of high importance such as CEOs, Board members, etc. Staff need to be vigilant when receiving requests from these people and challenge anything out of the ordinary – especially those dealing with finance. Adversaries may pose as the CEO and request that an invoice is paid.