Eastern Region Special Operations Unit

Regional Organised Crime Unit

COVID-19 CYBER & FRAUD PROTECT MESSAGES

Friday 24th April 2020

Today's topic is 'Social Engineering'.

We often hear about the attacker who uses technical expertise to infiltrate computer systems and compromise sensitive data, prompting organisations to invest in new technologies that will bolster network defences. However, there is another type of attacker who uses different tactics; they are called "social engineers" because they exploit the one weakness that is found in every organisation: human psychology. Using phone calls and other media, these attackers fool people into handing over sensitive information.

An example of social engineering
Secure Network Technologies were hired by a credit union to assess their vulnerabilities and conducted an experiment. Twenty flash drives, containing a Trojan virus, were left in the car park and other areas nearby. Once plugged in they collected passwords. Fifteen of the drives were found and plugged in by employees and the data started immediately flowing.

Increasingly sophisticated social engineering attacks can fool employees into divulging sensitive information or granting access to the wrong people. Here are a few of the most common social engineering techniques to be on the lookout for:

Phishing
Phishing uses a fake email from a third party to trick them into clicking on a link or providing sensitive information.
See our previous briefing for how to mitigate the risk.

Vishing
Vishing uses the phone instead of email. Scammers ask for personal information such as date of birth, address, financial information, etc.
Can you always trust who is on the end of the line? When in a conversation with someone you don't know, before answering a question make sure they need to know the information that they're asking about.

Pretexting
Pretexting is another form of social engineering where attackers focus on creating a good pretext, or a fabricated scenario, that they use to try and manipulate victims.
Don't get caught up in the story being told. A sense of pressure should be a red flag. Ensure that staff know what procedures they must follow e.g. urgent request to transfer funds.

Baiting
Received an email or text with the promise of a voucher for a free coffee or discount at a local store - what could possibly go wrong?
Unsolicited emails containing links should always be treated with suspicion and make sure your anti-virus is up to date.

Tailgating

Tailgating is used to gain access to a secure building by blending in and making you think that the hacker truly belongs there. Workmen wearing hi-vis often pass unnoticed in the work environment, why would they be there if they didn't need to be?
Educate staff to be on their guard. Look for ID and passes and encourage staff to ask strangers in the workplace who they are there to see.

What do we know about you?

Serious social engineers, will do deep background searches and reconnaissance on their targets before moving. This includes both verbal communication and social media like Facebook or Twitter.
Be aware of the information you are giving out and your digital footprint. Review your privacy settings.

Hot topics

Text messages are being sent to recipients, purporting to be from HMRC, advising they can get a tax refund of up to £400. The text features a link to a fake government website where the recipient can determine whether they are eligible for a refund.

Local reports have identified a phishing text message purporting to be from DVLA with a link to claim vehicle tax refund.

> *DVLA: Your outstanding vehicle tax refund from an overpayment is pending. Please visit our secure link to process https://dvla.ukgov-form1lt.com/?c=2*

Individuals are sent to a fraudulent looking .gov website asking for personal details including NI number, driver license number, mother's maiden name, debit card and bank details.

Another scam involves phishing attempts claiming to be from the UK Business Advice Bureau, offering government grants up to £25,000, aimed at small businesses. The email contains a telephone number, email address, and business address. Emails like this can be forwarded to the NCSC for action - report@phishing.gov.uk

Reports have been received of victims getting automated calls in which they were told that masks needed to be worn when leaving their residence and to press 1 to purchase one.

Reporting

Reporting to Action Fraud can be done online or by calling 0300 123 2040.
To report offers of financial assistance from HMRC, contact phishing@hmrc.gov.uk.

This advice has been collated by the East Midlands Regional Organised Crime Unit (ROCU) and is intended for wider distribution to raise awareness among businesses and the public.

Advice and information is changing daily as we navigate our way through the COVID-19 pandemic, so please ensure you only take information from reputable sources.

If you require any further information, assistance or guidance please contact the ERSOU Protect Team CyberProtect@ERSOU.pnn.police.uk or your local Force protect team.