Eastern Region Special Operations Unit

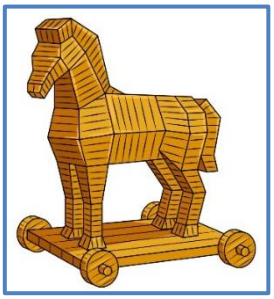
Regional Organised Crime Unit

COVID-19 CYBER & FRAUD PROTECT MESSAGES

Tuesday 5th May 2020

Today's topic is 'Social Engineering'.

According to the famous hacker Kevin Mitnick, social engineering is the *'the casual or calculated manipulation of people in order to influence them to do things they would not ordinarily do'*.



Social engineering may be the oldest type of attack on information systems, going all the way back to the original Trojan Horse - you could even say Odysseus was the first hacker to use Social Engineering to circumvent security.

Social engineering may lure the target into a false sense of security, encouraging or pressurising them to act without thought. Scammers may also seek a social connection or bond to add credibility.

Social Engineering 'slang' explained:

- **Blagging:** Convincing someone to hand over sensitive information or permit unauthorised access.
- **Phishing emails:** Encourage victims to download a harmful file, follow a link to an infected site or type in credentials so they can be captured and reused. Just as popular are fraudulent requests for payments.
- **Spear phishing emails:** These emails are entirely convincing because personal or organisational information is known by the attacker. This knowledge has been mined from publicly accessible records or internet sources, such as the company website or a social media profile.
- **Whaling emails:** Again this is no different from phishing, however the intended victim is someone with privileged access within a company or the ability to authorise transactions.
- **Vishing:** Ring up and convince the target to give away important personal data or credentials, or make a fraudulent payment.
- **Baiting:** This might involve leaving an infected USB drive where it might be picked up and plugged in (or in the case of Troy, wheel a wooden horse inside the fortress).

Solutions

Phishing emails, in their various guises, usually have tell-tale signs:

- Spelling, grammar or formatting errors all scream scam when the email purports to be from an official entity.
- Close inspection of the 'From' field might reveal subtle differences. **BCB.co.uk** is not the same as **BBC.co.uk.**
- Malicious files are often attachments that end in .exe or documents requiring macros to run.
- How does this email deviate from normal procedure? For example, are payments usually requested in this manner?

Vishing:

- No organisations will call and ask for credentials or request a payment.
- No matter how friendly or stressful the call might seem, ask yourself a) is this call expected? b) how can I contact the company or individual through official, well known, channels?

Keep an eye out for reported scams. Knowledge of attack methods and techniques will hone the ability to separate fact from fiction.

If you think you have been duped, change passwords run anti-virus and ask for help from a trusted source.

More detailed advice and guidance from the NCSC can be found here.

Hot Topics

Courier Fraud continues to be a problem in the region with several reports of elderly victims being targeted. This also presents a health risk to the victim, via physical contact with the scammers.

Criminals are using spoofing technology to send texts and emails impersonating known and trusted organisations. If you receive an unexpected text or email, asking for personal or financial details, do not respond and don't click on links or attachments in texts or emails.

Report SMS scams by forwarding the original message to 7726 (*spells SPAM on the keypad*).

Emails advertising the COVID-19 finger prick test for antigens have been confirmed as containing malicious links. Never click on links in suspicious emails.

Video conferencing is still being exploited with phishing campaigns targeting user credentials for both Skype and Zoom. One attack method used targets Skype credentials, the other leverages fake Zoom video-conferencing meeting notifications.

Webinar - Thursday 7th May 2020 @ 1400 – 1500 hrs

This week's topic: **Social engineering: Hacking the Human**

Internet of Things (IoT) devices feature in many homes, but are also increasingly integrated into industry infrastructures. This session, and the themes covered are applicable to both individuals and businesses.

To register for this event please visit Eventbrite.co.uk and search for 'National Policing'- places are limited.

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.