Eastern Region Special Operations Unit

Regional Organised Crime Unit

COVID-19 CYBER & FRAUD PROTECT MESSAGES

Tuesday 12th May 2020

Today's topic is 'Vishing'.

Vishing is actually a combination of two key terms 'voice' and 'phishing'.

Phishing uses deception to get an individual to reveal personal, sensitive, or confidential information, such as bank details or account passwords. Instead of using regular emails, or fake websites like phishers do, vishers use an internet based telephone.

An accomplished visher will 'spoof' a legitimate phone number in order to convince an individual that the call is from a legitimate source. They will then use a combination of scare tactics and emotional manipulation to get the victim to reveal information.

Some vishers will even mine publicly accessible records or internet sources, such as a company website or a social media profile in order to demonstrate knowledge of the target and improve the quality of the scam. When a visher cites a name, and or personal details, this implies that they have some form of legitimate connection to the target.

Common vishing exploits include calls purporting to be from the bank, credit card company, Inland Revenue, business partners, charitable organisations, insurance companies, debt collectors and technical support. The objective is nearly always the same - to trick you into giving sensitive information so they can access financial accounts or steal an identity.

Don't be a victim:

- **Keep abreast of the news:** Knowledge of attack methods and techniques will hone the ability to separate fact from fiction.
- **Understand:** A legitimate business won't make unsolicited requests for personal, sensitive, or financial information. Anyone who does this over the phone is probably trying to scam you.
- **Call back using official channels:** No matter how friendly or stressful the call might seem, ask yourself, 'how can I contact the company or an official representative through official, well known, channels?' Once you know the correct communication channels, verify the claims being made.
- **Don't give into pressure:** If someone tries to coerce you into giving them sensitive information, hang up.
- **Use Telephone Preference Service (TPS):** Register your number with the TPS to prevent unwanted sales and marketing calls.
- **Guard sensitive data:**
  - **Social media:** Think carefully about information appearing on social media posts.
  - **Unsubscribe:** from unwanted but legitimate emails.

- Remove your data from websites by using the **'contact us'** part of any web page. Under GDPR, everyone has the right to 'be forgotten' and can request the removal of their personal information. All organisations must comply with this.

- **Consider an App:** There are multiple apps that can be downloaded on a smart phone, to check incoming calls against a large database of known threats to forewarn you of potential problems. Always check the privacy permissions of any app installed.

Hot Topic

The NHS tracking app has generated debate over privacy and security concerns, however:

- The app does not collect your personal data so you remain anonymous.
- The app does not collect personal details of anyone you interact with.
- App data is encrypted.
- When anonymous data is uploaded to the NHS, the systems used are said to be secure. Not enough information is collected to specifically identify individuals.

Smartphone contact-tracking system(s) work by logging each time two people are within a certain distance of each other for longer than a specified amount of time.

When a user registers themselves as being infected, an alert is sent out to everyone they could have passed it on to. This is calculated by a risk based algorithm.

Further information on this topic from the NCSC can be found on their website.

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.