10 JULY 2020

WMCYBER@WEST-MIDLANDS.PNN.POLICE.UK
WWW.WMCYBER.ORG

GO PHISH!

Don't let the cyber criminals win by reporting it!

West Midlands | Regional Cyber Crime Unit

Cyber criminals love phishing. Unfortunately, this is not a harmless riverbank pursuit. When criminals go phishing, you are the fish and the bait is usually contained in a scam email, text message or via a social media communication. Phishing emails can reach millions of users directly, attacks can install malware (such as ransomware), sabotage systems, or steal intellectual property and money.

Organisations of any size and type as well as individuals can be hit. Mass campaigns is where the attacker is looking to collect passwords or make easy money, but a targeted attack against an organisation is where the aim is more specific, like the theft of sensitive data. In a targeted attack, the attackers may use information about an organisation or its employees to make messages more persuasive and realistic; known as **SPEAR PHISHING**.

HOW TO DEFEND AGAINST PHISHING

Defence against phishing often relies on users being able to spot phishing emails. Organisations should also widen their defence to include more technical measures.

• **Training** - Help by training users how to identify and report suspected phishing emails - Responding to emails and clicking on links is a part of the modern workplace. Spotting phishing emails is hard, and spear phishing is even harder to detect.

• **Additional Technical Defences** - Make it harder for emails from your domains to be spoofed by employing the anti-spoofing controls: DMARC, SPF and DKIM, and encourage your contacts to do the same.

• **Rapid Incident Response/Disaster Recovery Plans** -All organisations will experience security incidents at some point. Organisations need to detect them quickly, and respond in a planned way. Knowing about an incident sooner rather than later limits the harm it can cause. Protect your organisation from the effects of undetected phishing emails by having a plan to minimise and recover from the impact of undetected phishing emails. Please get in touch with WMRCCU at wmcyber@west-midlands.pnn.police.uk for help and incident response planning guidance.

• **Report it** - Check out the WMRCCU YouTube Live Video "Spotted a Suspicious Email? What to do with phishing emails. https://youtu.be/fOMbZsRILdc. The NCSC has launched the pioneering 'Suspicious Email Reporting Service', which will make it easy for people to forward suspicious emails to the NCSC – including those claiming to offer services related to coronavirus. Email: report@phishing.gov.uk

The NCSC provide more detailed advice on 'phishing', from the NCSC, can be found here https://www.ncsc.gov.uk/guidance/phishing.

Another phishing variation is **'WHALING'**, a highly targeted phishing attack aimed at senior executives masquerading as legitimate email. The emails contain personalised information about the targeted organisation or individual, convey a sense of urgency and are crafted with an understanding of business language and tone.

Using social engineering this can deliver huge returns without great technical knowledge and is one of the biggest risks facing businesses.

EXAMPLES OF COVID-19 RELATED PHISHING SCAMS:

The HMRC Phishing E-mail:
Purporting to be HMRC, it's offering claims made through the Coronavirus Job retention scheme, phishing for individual's bank details to provide COVID-19 relief payments. The email text is below and a link takes you to a web form, to steal your info:

Dear customer,
We wrote to you last week to help you prepare to make a claim through the Coronavirus Job Retention Scheme. We are now writing to tell you how to access the Covid-19 relief. Information you will need before you make a claim you will need to tell us which UK bank account you want the grant to be paid into, in order to ensure funds are paid as quickly as possible to you. You should retain all records and calculations in respect of your claims.

- A message is received (either email or through social media) from someone purporting to be a friend. The suspect uses the outbreak as a reason for requiring financial assistance. The victim transfers money to the suspect, believing it to be their friend.
- An individual is persuaded by the suspect to make an advanced payment for a rental property. The suspect uses the outbreak as the reason for the victim being unable to view the property. The property does not exist.