LET'S TALK PHISHING

CYBER SECURITY AWARENESS MONTH 2020

Phishing attacks aren't new and, unfortunately, they are probably here to stay. It's important to remember that when talking about phishing attacks, we are talking about a form of social engineering. These are sadly fairly successful as the attacker clouds the judgement of the victim with emotional tricks. When you receive a message or communication that you are not expecting and it asks you to do something and makes you feel emotional (rushed, happy, panicked, embarrassed or anything else) it is something to be wary of as this could be social engineering.

PHISHING, MORE THAN JUST EMAIL...

It is surprising to many people that phishing doesn't just refer to email phishing. Cyber criminals follow the numbers, the more popular a technology or app is, the more criminals will target it. Over the last few years there has been a serious increase in the following types of phishing:

- Email phishing
- SMS phishing: Via SMS message / messaging platforms such as WhatsApp
- Vishing (voice phishing): phishing over the phone
- Social media phishing: phishing through fake profiles on social media platforms such as twitter and LinkedIn. Click here to read our blog on Linkedin Phishing.

FUTURE THREATS

Internet of Things (IoT) phishing: social engineering attacks will almost certainly begin to target IoT devices. Remember, cyber criminals follow the numbers, the more popular IoT devices become, the more criminals will target them.

LET'S TALK PHISHING

CYBER SECURITY AWARENESS MONTH 2020

CASE STUDY: WHATSAPP

This WhatsApp attack is the perfect example of cyber criminals following the numbers. Since the start of the global pandemic, WhatsApp usage has rocketed globally by more than 40%. In the case of this SMS phishing attack, the attackers rely on an individual trusting a friend who needs help.

Below is the message someone in the Cygenta team received. Not only have the attackers places a sense of urgency on them, making them feel rushed, but the attackers have also used emojis to help normalise the message. Click here to find out how the attack works.

TOP TIPS FOR PROTECTING YOURSELF AGAINST THIS WHATSAPP PHISH

✅ Never send a 6-digit verification code to anyone for any accounts

✅ Enable 'Two-Step Verification' in WhatsApp

✅ If you are compromised, reinstall WhatsApp and get a new 6-digit verification code

✅ If you are compromised, change your Facebook password. Facebook own WhatsApp and your Facebook account could have been compromised before your WhatsApp one

LET'S TALK PHISHING

CYBER SECURITY AWARENESS MONTH 2020

TOP TIPS FOR YOU, YOUR FAMILY AND FRIENDS

- ✅ If you receive a communication that you're not expecting (whether by WhatApps, email, phone call, SMS message or any other way) that is asking you to do something and makes you feel emotional (rushed, happy, panicked, embarrassed or anything else), be aware this could be social engineering
- ✅ Legitimate organisations, such as your bank will not send you a text message asking you to share personal or financial information
- ✅ Avoid clicking links you're unsure of (clicking the link could infect your device) but instead go directly to the source
- ✅ If you receive a phone call asking for personal or financial information, hang up and call back on a number you trust
- ✅ Do not post your mobile number on social media and avoid giving it out when it's not required

CASE STUDY: TWITTER

This extraordinary hacking of celebrity twitter accounts is one of the biggest examples of vishing (voice phishing) we have seen. The criminals were able to obtain the phone numbers of a handful of Twitter staff, and through friendly persuasion were able to gain usernames and passwords which enabled them to access internal systems. From here they were able to compromise high profile accounts, which then enabled them to send tweets and access private direct messages. Twitter have said 'This was a striking reminder of how important each person on our team is in protecting our service.' We know your organisation will think the same of you, you are so important!