Shall we go Phishing today?

Just over a year ago I wrote an article on phishing scams, which are the way in which criminal use the internet and social media into deceiving victims into disclosing personal identities and login credentials. Given the increase we have seen in recent months at Safe Communities Portugal this updated article is timely.

Phishing respects no national or regional boundaries and we regularly receive information from people who have become victims or alerts from organisations that fraudsters are using their name to carry out such attacks. We alert people to this on our Facebook page.

In general, the goals of a phishing attack are to: obtain login credentials to be used to gain access to your assets; obtain other sensitive information, such as financial or personal data such as passwords, account numbers or social security numbers or transferring funds or convince the victim to carry out any other activity against their self-interest, such as transferring money or sharing personal data.

These can pretend to be well known organisation, everyday names such as EDP, CTT or emails in the name of someone you have never heard off.

There are several reasons why this type of threat is so dangerous. Firstly it is fairly inexpensive and easy to carry out. Perpetrators prepare mass mailings, hoping to lure even **just one victim** into giving out information or allowing access to a system. If you reply, that shows the scammer that your email address is active and you will receive more.

Some alarming statistics.

Phishing accounts for 90% of data breaches; 15% of people successfully phished will be targeted at least one more time within the year. The following statistics mainly from Symantec show that after declining in 2019, phishing increased in 2020 to account for 1 in every 4,200 emails. Phishing attacks account for more than 80% of reported security incidents and that US $ 17,700 is lost every minute due to a phishing attack.

Some of the increase may also be accounted for by the upsurge in COVID-19-themed email attacks.

Some Recent Examples received in Portugal

Criminals regularly use the name of **CTT** is such attacks. In one such case in the Algarve recently a person posted on social media.

“Yesterday we received an e-mail from CTT Expresso asking for a small amount of money to cover the customs tax on a parcel that was to be delivered. Normally, we would ignore something like this, but this week happens to be my husband's birthday and family members had told us they had sent parcels. So we paid it. This morning our Portuguese bank account had been all but cleared out”.

The person concerned was clearly the victim of Phishing. These are very common and in the case of CTT they regularly issues alerts to these.

The Portuguese Tax and Customs Authority (AT) in August last year warned of fraudulent e-mail messages using the “finance portal” address and urges taxpayers not to open the suggested link.

“The emails were from the portaldasfinancas.3aqb9 @ .pt address where they are asked to click on a link that is provided,” says AT, noting that “these messages are false and should be ignored.”

Sometimes these purportedly come from the police themselves such as an alert posted by the PSP recently:

“We warn of fake emails in circulation pretending to be from the **Public Security Police**.

Please be advised that this message is false and completely oblivious to PSP. It's a phishing message and should therefore be deleted immediately. If you receive an email of this nature, please pay special attention to provenance”.

Beware of Vishing

Vishing (a combination of the words Voice and Phishing) is a phone scam in which fraudsters try to trick the victim into divulging personal, financial or security information or into transferring money to them. In order not to fall victim to this: Beware of unsolicited telephone calls.

Take the caller’s number and advise them that you will call them back. In order to validate their identity, look up the organisation’s phone number and contact them directly. Don’t validate the caller using the phone number they have given you (this could be a fake or spoofed number).

Fraudsters can find your basic information online (e.g. social media). Don’t assume a caller is genuine just because they have such details. Therefore don’t share your credit or debit card PIN number or your online banking password. Your bank will never ask for such details. Don’t transfer money to another account on their request - your bank will never ask you to do so and lastly if you think it’s a bogus call, report it to your bank.

Prevention

Keep in mind that most reputable companies will not request personally identifiable information or account details via email. This includes your bank, insurance company, and any company you do business with. If you ever receive an email asking for any type of account information, immediately delete it and then call the company to confirm that your account is OK.

Do not open attachments from suspicious or strange emails — especially Word, Excel, PowerPoint or PDF attachments. Avoid clicking embedded links in emails, because these can be seeded with malware. Instead, visit the site directly by typing in the correct URL address to verify the request, and review the vendor's contact policies and procedures for requesting information. Hovering your curser over an embedded link with show the link’s URL.

Always remember to use virus protection and anti-spam software to protect yourself when malicious messages slip through to your computer. Watch out when using a mobile device. It might be harder to spot a phishing attempt from your phone or tablet.

More details at www.safecommunitiesportugal.com

David Thomas

President

Safe Communities Portugal

29th March 2021