Phishing – Don't take the bait

From time to time we come across various on-line scams as well as those which are received by people in the Algarve or sent to us at Safe Communities.

These take various forms, but the majority are what are known as "phishing" scams. In general, the goals of a phishing attack are the following: obtain login credentials to be used to gain access to your assets (an account, a server, a network or similar); obtain other sensitive information, such as financial or personal data; deliver a malicious payload (such as ransomware); convince the victim to carry out any other activity against their self-interest, such as transferring money or sharing personal data.

Phishing can be targeted at specific individuals (e.g. targeted spear phishing attacks) or sent to a large distribution of email addresses with a varying degree of tailoring (e.g. untargeted phishing attacks).

Untargeted phishing campaigns aim to reach as broad an audience as possible with the goal of tricking recipients into clicking a link, opening a malicious attachment, disclosing sensitive information such as passwords, account numbers or social security numbers or transferring funds.

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

Although phishing has been around for years, it continues to affect many users who still fall prey to tactics used to bait victims into disclosing personal identities and login credentials. Research reveals that the average Internet consumer is normally not aware of (or not particularly concerned with) phishing before having fallen prey to this type of high-tech scam.

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. Phishing attempts have grown 65% in the last year and almost 50% of phishing sites are using HTTPS encryption – a 40% increase over the previous quarter in 2018. More than 1.5million new phishing sites are launched each month (source Webroot). Phishing attacks have affected 76% of businesses in the UK; 30% of phishing messages are actually opened by targeted users and 12% of those users click on the malicious attachment or link. (Verizon).

Some Recent Examples received in the Algarve

We Transfer - Be aware that there are fake WeTransfer emails being sent. In one case the senders address was: sales (at) cargoonelogistics-com.ga. The email invited the recipient to click on a download link which was based in Russia. An obvious fake.

WeTransfer recommend various checks if you receive such an email which could be an attempt to steal your login details or install malware on your machine. In addition to more general advice they specially ask recipients to check if the layout different from the layout you usually see when you open a WeTransfer mail? Check the sender's address. WeTransfer always send their service-related emails from "…@wetransfer.com". If the email is sent from a different address, don't open the download link. Additionally they advise to check the address the email was sent to. They only ever send a transfer email to your own email address. Not to "undisclosed recipients" or to other addresses.

World Bank issued a press release in August this year asking individuals and businesses to take care not to fall victim to investment scams, known as Advance Fee Fraud schemes. Some of these schemes misuse are in the name of World Bank or falsely claim to be affiliated with the World Bank Group.

Advanced fee fraud schemes involve solicitations that encourage potential victims to provide personal information such as signatures or bank account information, and to pay certain advance fees, often described as "processing fees" or "finder's fees". In return, the potential victim is promised sums of money which the scammer has no intention of paying.

The Portuguese Tax and Customs Authority (AT) in August 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."

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.

David Thomas

Safe Communities Portugal

13th January 2020