Six tips for identifying malicious emails - blueAPACHE

Canonical: https://www.blueapache.com/blog/six-tips-for-identifying-malicious-emails

Details:

2017

In January this year, the Australian Tax Office (ATO) issued a warning regarding scam emails purporting to come from the ATO. The emails contained a link that when clicked had devastating effects; anything from installing keylogging spyware to CryptoLocker ransomware. This was followed in April, by reports of fake emails claiming to be from the Department of Human Services' myGov website. These emails were designed to capture personal information of recipients under the pretext of verifying their identity. Last month, the world witnessed a cyber-attack of unprecedented scale when the WannaCry ransomware was delivered to more than 230,000 computers in over 150 countries via an email containing a link or a PDF file with payload. The common factor in all these attacks? Email. While email scams and malwares have been in existence for a long time, their increasing sophistication and frequency is making them a top concern for many organisations. Moreover, modern email malware use evasion techniques designed to get around traditional security solutions. For instance, in the case of the ATO scam, each email had a unique link making it very difficult for anti-virus software to identify the bulk email as suspicious. Some email malware are so cleverly executed that at times it is difficult even for professionals to identify them. Termed as social engineering and phishing attacks, these malicious emails manipulate people into divulging confidential information or installing malware that can hold them to ransom. According to this year's Data Breach Investigations Report 1 in 14 users were tricked into following a link or opening an attachment – and a quarter of those went on to be duped more than once. Businesses today are entirely reliant upon emails for everyday communication and a single disruption can cost millions and destroy reputation. In spite of this, many users are not adequately trained on how to recognize phishing and ransomware attempts and often fall prey to them. Even with the growing sophistication of social engineering attacks, there are some basic rules that anyone can use to detect if an email is suspicious or not. How can you identify malicious emails? Here are a few questions to ask yourself to help determine if the email you have received could be malicious:

Who is the email from? An email from a legitimate address will often use the same address as the website. For example, an email from us would be from name@blueapache.com. However, an email from joe427@ato0989.org might indicate suspicious activity. You can view the sender's email address by clicking on the name or hovering over it.

Is the email unsolicited? Is it from an organisation that you do not normally deal with or are not expecting to hear from? If it mention flights you may have never booked, parcels you did not send or refunds you are not expecting, then be very cautious. If possible, contact the sending organisation to confirm if they sent it to you.

Does the email contain external links? If the link says one thing but points to a different server, it is likely to be malicious. One way to check this without clicking the link is to hover your mouse over the link. A pop up will show you where the link redirects to.

Is the website domain not quite right? Fake domains closely resemble actual ones, but will have small differences – for instance, www.linkedlin.com or www.facbook.com. http://www.whois.com/whois/ is a free service that you can use to find who the domain is registered to. It only takes a few seconds to use and could save you weeks of inconvenience.

Does the email contain any attachments? If the attachment is a file with a .exe, .cmd or .bat extension, it could be a malicious program that will install code onto your computer when run. Check with the

sender if the file was sent by them and what it does upon running.

Do the graphics look different? Scammers try to imitate real organisations as closely as possible by using the same logo, graphics and colours, but it will often be of poor quality. When poorly executed, some of them also contain spelling or grammatical errors. What should you do if you have received a malicious email? If you think the email you've received could be malicious, get an expert to check it out. Do not reply or forward the email, do not click on links or open attachments contained in the email. If you do suspect you have fallen victim to an attack then log off and shut down your computer immediately and contact your IT support to minimise the impact. To better understand how you can protect your organisation from email malware, contact your blueAPACHE account manager .

What is the topic of your article 'Six tips for identifying malicious emails'?

We discuss how to identify malicious emails, referencing real-world scam examples such as fake Australian Tax Office (ATO) emails, fraudulent myGov emails, and the WannaCry ransomware attack, and provides six practical tips for spotting suspicious emails plus advice on what to do if you receive one.

How did the WannaCry ransomware attack spread ?

The WannaCry ransomware was delivered to more than 230,000 computers in over 150 countries via an email containing a link or a PDF file with a malicious payload.

what statistic illustrates how often people fall for phishing links or attachments?

According to that year's Data Breach Investigations Report, 1 in 14 users were tricked into following a link or opening an attachment, and a quarter of those went on to be duped more than once.

How can you check where a link in an email actually leads without clicking it?

You can hover your mouse over the link, which will show a pop-up revealing where the link actually redirects to, without needing to click it.

What should you do if you think you've received a malicious email?

If you think an email could be malicious, you should get an expert to check it out, and you should not reply to or forward the email, nor click on links or open attachments in it. If you suspect you've already fallen victim to an attack, you should log off and shut down your computer immediately and contact your IT support to minimise the impact.

Who should you contact to learn how to protect your organisation from email malware, ?

We advise contacting your our account manager to better understand how to protect your organisation from email malware.

Why are modern email malware attacks difficult for traditional security solutions to detect?

Modern email malware uses evasion techniques designed to get around traditional security solutions. For example, in the ATO scam, each email had a unique link, making it very difficult for anti-virus software to identify the bulk email as suspicious.