Spotting a suspicious sender

When examining an e-mail for phishing scams it is crucial to consider both the overall context and the finer details. Specific elements within the message can provide indicators of a phishing attempt. When opening an e-mail remember to pause and evaluate. Ask yourself, does this e-mail make sense? Should I be receiving this e-mail from this sender at this particular address?

Phishing clues in the sender's address

The sender's e-mail address can be a key indicator of a phishing attempt. It's crucial to focus on the actual domain in the sender's address not just the displayed name. An e-mail domain shows which organisation or service manages the e-mail account.

This is important because cyber criminals use domains that closely resemble legitimate ones to deceive recipients into thinking the e-mail is from a trusted source. The ability to accurately identify the domain in a sender's address will thwart a large percentage of phishing attacks.

Follow these two simple steps to identify an e-mail's domain. We'll use this e-mail as an example: alerts@equifax.com. The first step is to find the end of the sender's address. In Step 2 identify the previous two sections from the end of the address. Here the previous two sections are 'equifax.com'. This is the true domain of the sender's address.

Now let's look at another example: support@verizon.security.com. The steps are the same. First, find the end of the sender's address. Then identify the previous two sections. Here the previous two sections are 'security.com'. This is the true domain of the sender's address.

By following these two simple steps you can accurately identify the domain in a sender's e-mail address and protect yourself from phishing attacks. Let's consider a few real-life examples relying on the sender's address to determine whether an e-mail is safe or suspicious.

Example 1: benefits@hr.alerts.com. Here by including 'hr' as a sub-domain the hacker hopes you'll quickly read the sender's address and trust the e-mail. However a legitimate e-mail from your HR department would come from a company account. The domain here is 'alerts.com' an unfamiliar and generic domain. This e-mail is suspicious.

Example 2: security@tvvitter.com. In this second example, the fraudster is hoping you'll confuse 'tvvitter.com' with 'twitter.com'. This is a common tactic where cyber criminals register domains that resemble legitimate companies.

E-mail addresses can be deceptive. Remember to analyse the sender's address not just the name of the sender. Identifying the domain name will help you determine where the e-mail actually came from.

Stay vigilant and report any e-mail that seems off. Remember to pause, evaluate and report.