Email Spoofing - Are they really who they say they are?

Email spoofing is the forgery of an email header sot that the message appears to have come from someone or somewhere other than the actual source. Spoofing is the tech equivalent of putting on a disguise to trick people into thinking you're someone else. It's amazing that in this day and age, with our tech-infused lives, the most effective cyberattacks rely on the oldest tricks in the book.

Spoofing someone's email is used to bypass security filters, by pretending to be from a trusted source. People are more likely to open an email when they think it's been sent by a legitimate source. It is a key component in phishing emails sent to users daily in efforts to steal their sensitive information. It is pretty simple for hackers to spoof email addresses. Cyber attackers can simply change the sender's address in an email to look like the message was sent from someone the user trusts. They can send an email to look like the message is from a coworker.

For example:

jjdoe@kent.edu is the actual coworker's email address. However, if you check the sender's actual user domain, you might see jjdoe253@kent123.com. In this example the only clue that you're looking at a spoofed email may be, the jjdoe253@kent123.com. It should be deleted and/or reported using a new technique provided on SecureIT.kent.edu. This is one way to prevent falling victim to a phishing attempt.

Phishing emails are becoming more sophisticated, follow basic security measures daily when going through your email:

- Check for wording that tries to get a quick emotional reaction, such as **URGENT** and **ACCOUNT CANCELATION**. Phrases such as these often appear in the subject line.
- Watch for typos and grammatical errors.
- Hover over any links to check where the link leads.
- Be cautious of any email that requests personal or confidential information, or some form of money/gift card transfer.
- If you receive a suspicious email that purports to be from someone you know, start a new email to contact them to verify its authenticity.
- Stop and ask yourself if this is the type of email you would normally receive from the sender.

Don’t let Black Friday and Cyber Monday become Bank Fraud and Cyber-theft Tuesday!

The holidays are fast approaching and buyers everywhere will be scrambling to find the lowest prices, the best gifts online. This time of year is the perfect time for cybercriminals to take advantage of unsuspecting online shoppers. Precautions need to be taken whether you’re shopping online from home or your mobile phone.

Black Friday and Cyber Monday are approaching quickly. Last year $5 billion was spent in 24 hours on Black Friday alone. No wonder Black Friday is also the biggest holiday for phishing scams! Fraud attempts are expected to increase this 2018 holiday season between Thanksgiving Day and Cyber Monday.

Online shopping has become an easy way to search for deals, and have them shipped quickly. The availability of online shopping has made finding great deals, making purchases and next day delivery very popular. While this is very convenient, it also makes it extremely lucrative for scammers to trick buyers into paying for something they will never receive and obtaining their personal information for financial gain.

Be cautious when looking at email offering you great deals! Online shopping scams are real and involve scammers pretending to be legitimate online sellers, either with a fake website or a fake ad on an actual genuine retailer’s site. The biggest tip-off that a retail website is a scam is the method of payment. Scammers will often ask you to pay using a money order, pre-loaded money card, or wire transfer, but if you send your money this way, it’s unlikely you will see it again or receive your purchased item.

Cybercriminals are taking advantage of your enthusiasm and anxiety with false tracking updates, and fake order confirmation emails. Don’t let the holiday stress distract you into being duped by an email pretending to be a well-known delivery service such as UPS, FedEx etc. If the email asks you to download an attachment or click a link, don’t do it! If you are expecting a package, call the company to confirm status updates.

A newer version of online shopping scams involves the use of social media platforms to set up fake online stores. They open the store for a short time, often selling fake branded clothing or jewelry. After making a number of sales, the stores disappear. They also use social media to advertise their fake website, so do not trust a site just because you have seen it advertised or shared on social media. The best way to detect a fake trader or social media online shopping scam is to search for reviews before purchasing. But even those can be faked, be cautious and do research. It is important to take steps to protect yourself when shopping online. Be security aware!

Click here for tips on protecting yourself and staying safe while online shopping. Take time to learn how to make your shopping online safer, and have a happy, safe and secure holiday season!

If you keep these tips in mind along with the usual precautions of unique passwords and login credentials for each site, you will be able to safely enjoy the cyber deals this holiday season. Take time to make your shopping online safer, and have a happy, safe and secure holiday season!