(Approx. 1089 words)

‘Tis the Season for Fraudulent Email

By David Kretchmar, Computer Technician
Sun City Summerlin Computer Club
https://www.scscc.club

dkretch (at) gmail.com

You have probably already received emails that appear to come from a bank or other online service requesting that you verify account credentials. You might have been asked to provide personal information including account and credit card numbers and passwords. This is a standard **phishing** technique; oddly, the sender is asking for information they should already have.

***“If you can’t spot a phishing email, you could be the next victim.”***

Unfortunately, during the COVID-19 pandemic, we’ve seen once again that phishing lures are mutating and they’re often hard to recognize.

Phishing is a form of social engineering email attack in which the sender tries to gain access to login credentials, to get confidential information, or to deliver a virus. This is accomplished by tricking humans like you and me.

Scammers know there’s a good chance that any message will be scanned for malicious content by the security software of your browser and mail provider. Google, Edge, and most other browsers are pretty decent about stopping known spam, but plenty still gets through. Scammers are constantly changing techniques.

Since the coronavirus pandemic started to unfold, fraudsters have wasted no time in trying to profit from the uncertainty and fear connected to the crisis. In March 2020, when this all started, there was a flood of COVID-19 themed spam, spreading malware, phishing for sensitive information, or offering bogus products.

According to Google, scammers were sending 18 million phishing emails about COVID-19 to Gmail users every day in March, which Google blocked. In April Google was blocking more than 100 million phishing emails a day. And these are just the phishing emails the tech giant blocked. Yet some still appear in your Inbox, and If you can’t spot a phishing email, you could be the next victim.

It is no surprise that the coronavirus pandemic has become a top subject for attackers. The appearance of any crisis brings new circumstances that provide a new environment for cybercriminals to innovate. At the same time, phishing attacks have also benefited from the number of new remote workers.

## So how do you recognize suspicious emails?

**Look at the sender email address**

The sender’s email address is the first place to look. If it looks “funny” or unfamiliar be careful with that message. You can check the email address by hovering your mouse over the ‘from’ address *but don’t click*. Scammers’ email addresses used to be anonymous or had very generic names with many numbers. Sometimes the sender’s email address wouldn’t match the sender’s name or the body of the message.

Receiving emails about a problem with your account from financial institutions with whom you have no relationship is a laughable tell. But if you do get an email claiming to be from your bank, closely review the email address. The email address is sometimes the only sign of a scam, due to how professional the messages look. If you feel the email might be legitimate, check your account the way you would normally access it (not a link provided in the email).

Keep in mind that any big outfit is going to have an eponymous address i.e., you contact PayPal at an address that includes paypal.com.

**Be suspicious of attached files or unfamiliar links**

Cyber criminals’ emails might contain malware or send you to a malicious web destination. If you are at all suspicious, don’t click. Legitimate service providers don’t send messages requesting you to log in via an embedded link. Also, pay special attention to attached files – once they are opened, these attachments can install malware to give someone else control over your computer. They can then initiate attacks on other computers, including by sending spam (often infected) to every contact in your address book.

**Watch for poor English**

Poor grammar or words used in an unusual way are possible indications of phishing. Always be suspicious; looking for unusual language and vocabulary, or misspelled words can help prevent you from becoming the next victim. Poor spelling and other grammar mistakes are common with phishing emails that have been translated from other languages. This kind of clue is less common today because the quality of social engineering has improved, so you are likely to receive a more professional presentation. Another thing that can signal an attempted attack is generic greetings such as "Dear recipient" or " Dear friend".

There’s sometimes a purpose behind misspellings and poor syntax. Cybercriminals most successfully prey on uneducated computer users, knowing them to be less observant and therefore easier targets.

**Is it too good to be true or is it frightening?**

Social engineering focuses on two human weaknesses, fear and greed. Does the email promise you a windfall of cash? Does it suggest you inherited a fortune or will be paid a fortune to help someone move money out of their country? Here’s an idea: Google for the same message, or a key phrase from that message. (highlight, right-click, search Google). You'll often see that many other people have received the same or similar fraudulent message.

Would-be cybercriminals using social engineering methods are very opportunistic. For example, this time of the year the names of shopping websites such as Amazon and Mayfair are used in sending out millions of emails claiming issues with your account or recent order and asking for personal information. They know consumers are most likely to have made purchases this time of the year.

The scammer wants to panic you into doing something. Don’t be threatened by an email. Does the message urgently ask for help or otherwise appeal to your emotions? These are common techniques. Do not respond to an email threatening to suspend your account if you do not answer in a short time.

**Homoglyph attacks**

Homoglyph attacks rely on replacing characters in addresses with ones that look similar, or are the same, but belong to different alphabets. These attacks are extremely dangerous for users because there is a very limited chance of detecting the trick. Like the attack on PayPal users in which the address contained the “correct letters” taken from our Latin alphabet – with two exceptions. The attackers replaced both instances of the letter P with a “P” look-alike letter, but from a different alphabet. This “P” look-alike letter was taken from the Russian alphabet, where it is equivalent to the letter R. With this kind of attack, you are dependent on the other clues discussed in this article to protect yourself.

