UC San Diego
UC San Diego News Center

By Lance Roberts and Christine Clark Mar 02, 2017

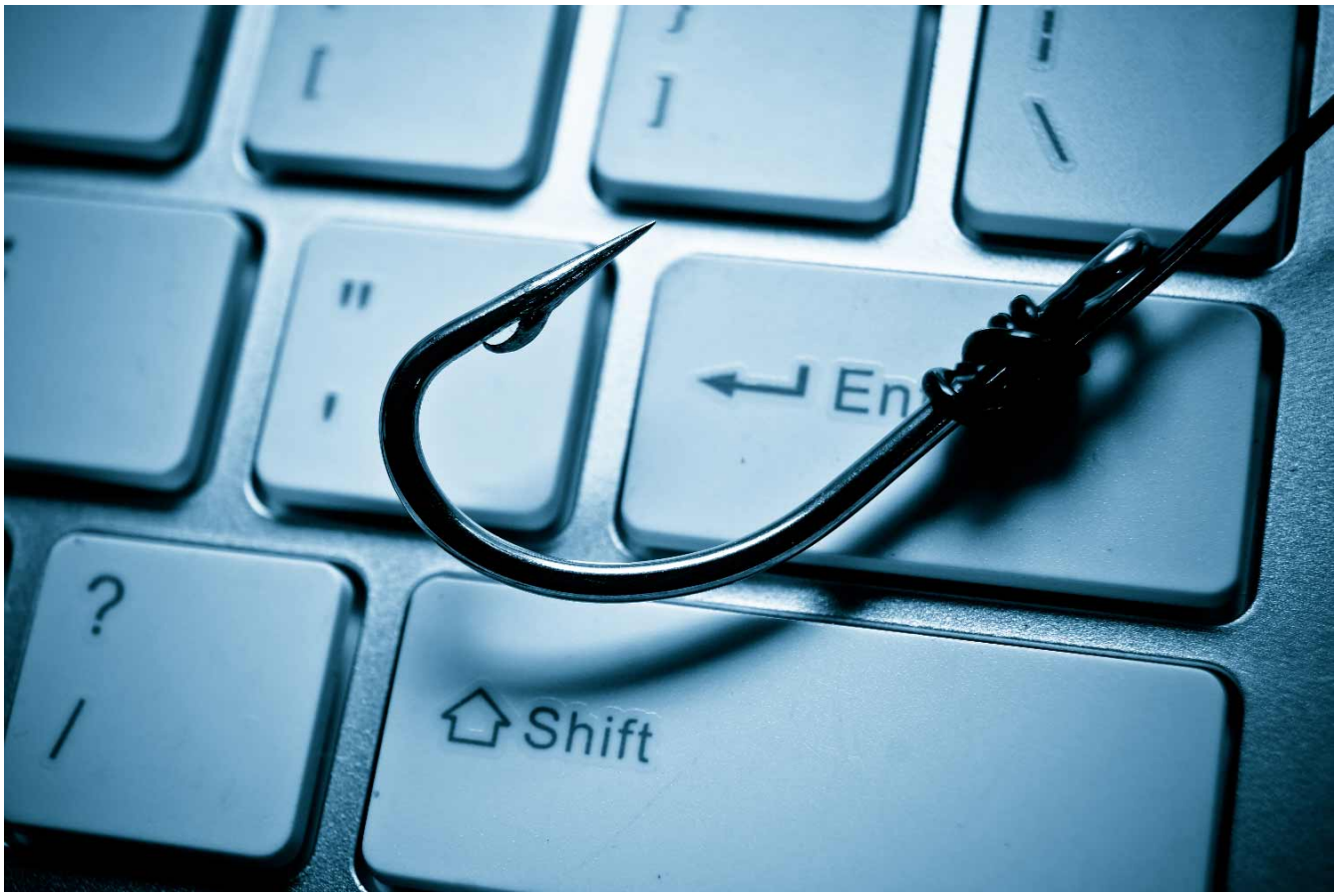

Photo by iStockphoto.com/weerapatkiatdumrong

Don’t be the Phish on the Spear: Tips on How to Prevent a Cyber-Attack

As every UC San Diego student, staff and faculty knows, emails come in by the tens or even hundreds on any given day. Some of those emails may appear to come from familiar sources such as a bank, social media, friends or even colleagues, but they may look odd or suspicious. These emails can range from a UC San Diego message indicating mail support for Internet Explorer IE 8 will discontinue to a “delivery failure notification” email from the U.S. Postal Service. What they are in reality, however, is a phishing scam.

The scammer's goal is to use our dependence on mobile phones, tablets and computers to obtain personal information that can be sold, used to access bank, credit card or medical accounts, or for identity theft purposes.

A phish is an email scam designed to acquire sensitive information from people, and these emails are most successful when they appear to come from a reputable source. The number of circulating phishing scams continues to grow, and no one is immune from being impacted by them, including members of the campus community. That is why the campus's Information Technology Services (IT Services) is promoting Cybersecurity Awareness throughout 2017. Each month, IT Services will publish articles, cybersecurity tips and updates on current threats. The goal is to help prevent cybersecurity issues before they happen or minimize the impact on faculty, staff and students. Though phishing scammers are becoming more sophisticated, here are some tips to avoid falling prey to a cyber-attack:

IT Services recently posted an easy to follow guide "How To Identify Phishing Scams."

Identify Phishing Scams:

- **Spear phishing** is directed at specific individuals or companies, usually via email or direct messaging. What makes these types of scams difficult to detect is they appear to be from a legitimate source and attempt to secure an individual's personal information using a fake website or infect their device with malware. Spear phishing was the primary way individuals in the 2016 presidential campaign were hacked.
- Another phishing method scammers use, often referred to as "clone phishing," involves copying a previously delivered email which included a link or attachment where they use the content and recipient address to create an identical email. The scammers then replace the attachment or link it with a malicious version and then send it from an email address made to appear that it came from the original sender.
- **Look for irregularities**: Often times, phishing emails include misspellings, unnecessary capitalization and other types of irregularities that point to an email being a phishing email.
- Other examples of fraudulent emails that appear to come from UC San Diego, UC San Diego IT Services or some other UC San Diego department:
    - Your email account is over quota.
    - You must click a link to reactivate or update your account.
    - You must provide your user information to keep your account active.

The Federal Trade Commission (FTC) offers a number of examples of potential phishing messages that might otherwise seem legitimate:

- “We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity.”
- “During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information.”
- “Our records indicate that your account was overcharged. You must call us within 7 days to receive your refund.”

Additional examples of potential phishing scams include:

- Misspelling of the company name or substituting the number “1” for the letter “l” in a web address (paypa1.com instead of paypal.com).
- Using http instead of https when the company’s actual URL uses https (the "s" stands for secure). The Anti-Phishing Working Group reports that a single phishing site may be advertised as thousands of customized URLs which all lead to the same attack destination.
- Pop-ups that immediately ask you to enter your username and password. Phishing scams may direct you to a legitimate website and then use a pop-up to gain account or personal information.

Report Phishing Emails

IT Services Security team supports the secure use, processing, storage and transmission of digital information and media among the UC San Diego community, including faculty, staff, students and affiliates.

- If you believe you are the recipient of a phishing email, you can forward it to abuse@ucsd.edu. There is a very good chance you are not the only person to receive the phishing email. By forwarding it to the IT Services Security team, you help reduce the potential risk to others.
- For additional information on how best to keep your data secure, visit the UC San Diego IT Security page periodically for updates: UC San Diego IT Security.

Protect Yourself from Phishing Threats

There are a number of steps you can take to protect yourself from a phishing attack. Here are some easy steps to protect yourself, your personal information and your accounts:

- Don't email personal or financial information.
- If you do need to provide personal information, make sure you typed in the web address yourself and you see signals that the site is secure, like a URL that begins https.
- Where possible, set up your email with a preview pane to view the message and the sender address without having to open the message. If the message doesn’t make sense, contact the

sender via a separate email to confirm they sent it to you.

- Always be cautious about opening attachments and downloading files from emails, even if you believe it is from a trusted source. These files can contain viruses or other malware that can weaken your computer's security.
- Install and update anti-virus software. Make sure all of your computers are equipped with regularly updated antivirus software, firewalls, email filters and antispyware.
- Be wary of hyperlinks: Avoid clicking on hyperlinks in emails; type the URL directly into the address bar instead. If you choose to click on a link, ensure it is authentic before clicking on it. You can check a hyperlinked word or URL by hovering the cursor over it to reveal the full address.
- Use the campus spam preferences tool which enables the quarantine that catches phish along with spam so it isn't delivered to mailboxes: http://blink.ucsd.edu/technology/email/spam/.

Keep up with campus news by subscribing to *This Week @ UC San Diego*