The CYBER GURU

Volume 6 **March 30, 2018**

Phishing: A Use Case at SDCOE

by Ed Kipp

Phishing is part of our cybersecurity presentation that we hit the hardest. We demonstrate what can happen if a link or attachment is clicked and a webcam is compromised. It always gets the audience's attention. We also give tips and tricks to spot phishing and encourage users to send suspicious emails to us. During a typical week at SDCOE, we might get two or three malicious emails sent to a handful of people. But the last week of February proved to be anything other than a typical week.

A little after 8 a.m., one of our users sent us a phishing email. We ran a message trace, inputting the sender's email address to find out who got the email. It was only two people. We asked them to let us know if they clicked the link. Then we blocked further emails from that sender and prevented anyone from accessing the link.

Unfortunately, the other user who received the email clicked on the link before we blocked it. When this happens, the best practice is to wipe the computer, because we are not sure of the damage. I have tried manually removing malware that would recreate itself as a randomly generated filename immediately after I deleted it. The only way to be sure something malicious isn't hiding is to start over. We requested that the machine to be reimaged and asked the user to shut down to prevent spreading or pivoting.

However, the person who sent the phishing email quickly took advantage of the vulnerability. One of the first things they must have done is download a local copy of the user's mailbox information. This gave them a list of everyone the user had emailed or received email from. The attacker took that information and started sending emails on a scale we have never seen before at SDCOE -- 3,575 over the next four days. It's possible the attacker was trying to keep the Cybersecurity team busy while they tried to take advantage of another vulnerability.

The following day, the user who clicked the link received an email that looked like a reply to an email chain from someone at a local school district. The email directed the user to send money to a different financial account, claiming that the correct account had be compromised. The email address looked very similar to the actual email address but was one letter off. Email addresses that have different domains are as different as Paris, France, is to Paris, Texas. Thanks to training and expertise, no money was transferred.

Within 24 hours, the phishing had compromised the machine, grabbed the contact list, looked through emails to find one that could be altered with fake bank information, created a bogus domain that looked legitimate, and bombarded us with phishing to keep us occupied. It could have been much worse. We took the opportunity to refine our processes and learned quite a bit from the experience. This is just one example of what can happen with something as simple as a click. We are working hard to make our processes more efficient and to reduce as much of the danger from phishing as we can.

Tips

Every month, we will bring you some of the most useful tidbits of information with how-to guides, fliers, and links to some of our favorite cybersecurity resources, which can also be accessed on our website.

- This month's **recommended websites**: Is this Website Safe? (Norton Anti-Virus), Test a Site (Palo Alto), and Test a Site or File (Forcepoint)
- This month's **flier**: Spring Break Road Trips?

Quick Tip

Watch for Phishing Clues: The majority of phishing attempts using email and text messages will have the same red flags: typos, mismatches between the stated link and the actual URL, an unknown sender, or a threatening sense of urgency. Become familiar with these clues to avoid falling victim to phishing.

Events

Our mission is to empower all of San Diego County to be cyberaware. Use our online events calendar to find out about awareness events happening each month.

- **April 9**: Online Safety and CyberCareers at Vista High School
- **April 13**: Social Media Safety and CyberCareers in AI/Machine Learning at Morse Senior High School
- **April 26**: Happy Half Hour with the Cybersecurity team
- **April 30**: Cyber Guru Volume 7 Released
- **May 2:** Train-the-Trainer: Data Security Awareness [Register]
- **May 2**: Train-the-Trainer: Hacking Demo [Register]
- **May 16**: Train-the-Trainer: Data Privacy [Register]
- **May 30**: Train-the-Trainer: Social Media Safety [Register]

Want us to speak in your K-12 or College classroom? Contact us today!

Security is everyone's responsibility.

SecuringInfo@sdcoe.net | 858-292-3626 | sdcoe.net/cybersecurity
Awareness | Procedures | Training | Vulnerability Assessment

Get up-to-the-minute information about what's happening at SDCOE and in our districts across the county.