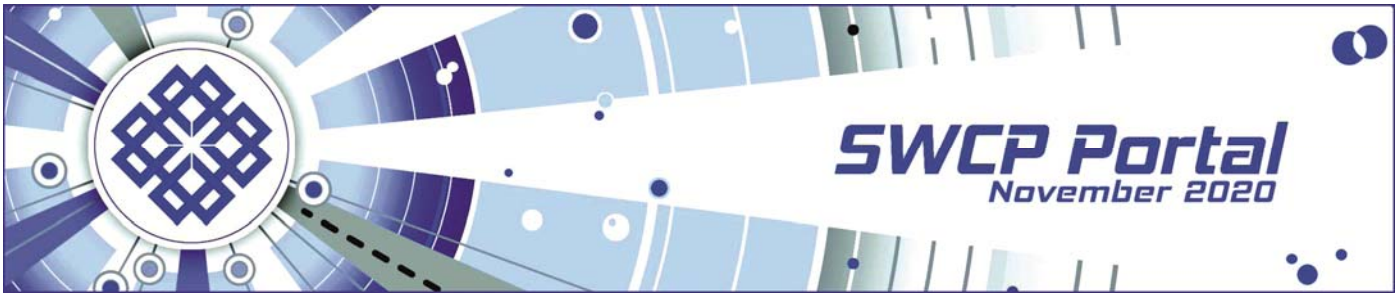

And just in time for the holidays.

Business Email Safety

Mark Costlow, SWCP President

It's all your fault.

Well, maybe not your fault, but you're the only one who can fix it.

After three decades running Internet Email servers, I have come to an unexpected, distressing, and perhaps unpopular conclusion: **Email users must protect themselves.**

The only true defense against determined social engineering techniques is awareness and vigilance on the part of the scam target.

From the very beginning, opportunists have used email to line their own pockets or stroke their egos. Spam was the first and most obvious scourge, followed by vandalism in the form of destructive email viruses. Within a few years, social engineering scams had taken hold. They are still with us, and getting worse.

In the old days, spammers spewed millions of identical messages. We pour time and money into blocking the junk, but feels like a bearable situation. Like a chronic disease with no cure, but treatments ease the symptoms so we can get on with life and business.

Social engineering scams, such as phishing and spear-phishing emails, are a different story. The consequences if we allow a spam into your mailbox are small – you have to click "`Delete`" one more time. But Phishing scams cost real money.

Phishing for a whale of a payoff

Phish emails are usually generic. They might claim to be from Google, Apple, or Facebook, and say you need to change your password. But if you click the link, it doesn't go to Apple or Google. Instead, it takes you to a **look-alike site**, which tells you to enter your old password to prove your identity, and captures that info and turns it over to the scammer.

That sort of phishing email can work on anybody. The criminals don't have to know anything about you. A small percentage of people take the bait, turn over their account credentials, and the bad guys steal your money, hurt your reputation, feed political misinformation campaigns, etc. The criminal gain from each target is relatively small, so they need a lot of them.

By contrast, Spear-phishing scams are targeted at YOU, or someone very like you. In fact that's where the term comes from. Fishing (in the outdoor rod-and-reel sense) is casting some bait and hoping a fish will wander by and get hooked. Spear Fishing is much more focused. The hunter is throwing that spear at a specific fish, hoping to bring home dinner.

Spear-phishing emails are usually missing the old tell-tales like broken English, foreign-sounding addresses, or wildly unlikely stories. They often reference people in your company by name. Some of those people might even appear to be CC'd on the message. And often the sender is someone you know and trust (like your boss, your CEO, or your counterpart at a another company).

Willie Sutton reputedly said he robbed banks because that's where the money is. Spear-phishers target business users because they have access to financial instruments on a much larger scale than most individuals.

We would need a lot more space to list all of the methods these scammers use, or the ways we can be tricked. So instead, we will relate one nightmare (true) story, including the methods used and the consequences. The names have been changed.

ABC Construction Company was expecting payment for a civil building project. It was supposed to come in two monthly payments of around $400,000 by electronic bank transfer. When the first payment was a week late, Jack (`jack@abc-construction.com`), in charge of Accounts Receivable contacted the city's Accounts Payables person Jill, (`jill@citygov.net`) to ask after it. Jill's response was, "We sent it on the first! You didn't get it?"

Investigation soon revealed that the month before, the city had received an email from jack@abc-construct1on.com, informing them that ABC Construction had made some banking changes, and please update their wire transfer details accordingly. Someone at the City received that email, which they thought was from good old Jack who they knew and trusted, so they changed the settings in the purchasing system so ABC would get their payment at the new "correct" account. They didn't realize that the mail came from the wrong domain name (notice the number "1" in the jack@abc-construct1on.com).

It only took a day to unravel what had happened, but by that time the money was long gone. The account it had been transferred to already no longer existed and the money had been moved along its laundering path.

Clearly this type of scam takes considerable preparation. The scammer had to know about ABC, and the City, and their relationship. They probably had already infiltrated the email of one of the organizations through previous phishing attacks. They were able to register look-alike domain names in advance, and construct emails with the right "voice", signatures, logos, etc. When the payday is $400,000, the scammers are willing to put in a bit of work.

These kinds of scams have been around for as long as there have been businesses. The difference is the electronic age gives criminals a vastly larger pool to choose from.

How could this have been prevented? There are not many technological fixes that would help. Remember that the email from ABC wasn't from ABC at all. We've collectively put huge resources into preventing someone from forging a message using someone else's real domain name. But that doesn't stop look-alike domains. Nothing in ABC's email system could have stopped this message between two other parties (the criminal and the city).

So this is how I got to that disagreeable conclusion: The person who was best positioned to prevent this theft was the one who received the fake email from abc-construct1on.com. If they had noticed the funny spelling, that might have triggered an alarm. But expecting humans to catch problems like that is not realistic.

What is realistic is to put more safeguards on the action that allowed the theft. In this case, changing the account details for a vendor in the purchasing system.

If you run a business, consider whether it should be possible for a single person to make those changes. If the potential dollar amounts are large, maybe require two or more people to approve the change. Or require a second validation before making the change (a phone call to Jack would have set off all the alarm bells in this situation).

Do not ever be afraid to ask the question. If you're dealing with money, nobody in their right mind will be offended or put out if you ask for verification on legitimate requests. Better to slow down every such change by a little bit than to risk it all by assuming there are no bad actors in the system.

Hopefully just being aware of these scams is an inoculation of a sort. If you receive an email requesting an account change, and it's not something you expected or knew about from other channels, question it.

But in addition to that, if **you** are responsible for avoiding scams, how do you do that? One way is to get better at spotting suspicious messages. Keep in mind that the tricksters are only going to get better at the fakes, so we need to up our game to spot them. Here is a quick **Phishing Quiz** via Google that you can take which demonstrates many of the techniques used by these criminals: (**https://phishingquiz.withgoogle.com/**) Try it out and let us know how you scored!

Right to repair moves forward

Massachusetts just passed a landmark law requiring car manufacturers to let people access their car's data by 2022 (**https://bit.ly/3l23wZ1**). Car-makers will have to develop and implement a standard **open data platform** that will allow owners and mechanics access to technical data called "**telematics**". By controlling that data, car-makers could severely limit third-party repairs.

Extending a 2012 law, this may lead to national standards which could be significant, as **right to repair** may become a very big issue, for firms like Apple guard their wares against outsiders with all the tenacity of a fire-breathing dragon.