SWCP Portal

February 2024

Forewarned, Forearmed

By Mark Costlow

Scams and social engineering have been around for millennia, from the **first documented insurance scam in 300 BC**, to the guy on craigslist collecting damage deposits from prospective renters for **houses he doesn't own**. Technology, and the Internet especially, makes us vulnerable to vastly more scammers than past generations. My great grandfather may have encountered 4 or 5 scammers in his lifetime, whereas I can see that many in a single day.

As a technologist, I once believed technology could solve most problems, especially the ones created by technology. However, when it comes to scams and social engineering, I did not fully account for the human element. Spam filters and anti-virus programs can never perfectly prevent their users from seeing some of the malicious things that scammers throw their way. Many big data breaches are not caused by a significant lapse in security systems, but rather by a **single human clicking something they shouldn't** or **unknowingly sending critical information to a criminal**.

This is not to say we should stop fighting criminals with security systems. We must continue that arms race. But we must also recognize that no system will protect us from our own naïveté. With that in mind, we present examples of scams that currently plague us. They come as email, texts, phone calls, and pop-up messages and they all have one thing in common. They want to exploit your lack of knowledge for their gain, and they don't care if they ruin lives in the process. Hopefully seeing what these scams look like will cause a little bell to ring in the back your head when you encounter one in the wild. Like using a vaccine to train your immune system to recognize a new pathogen, we want to inoculate you against these dirty tricks.

Email Scams

Shame extortion scams try to convince you that they have some dirt on you, and if you don't pay they'll send it to your friends and family. They claim to have installed a virus on your computer and have access to your keystrokes and webcam. These are things that could happen, which lends credence to their claims. They often include some personal information to make it even more convincing, usually a password of yours which you might recognize. They get the password (and your email address) from a **data breach** and don't actually have any current knowledge about you.

Speaking of **data breaches**, they are why we must use different passwords on every web site or service. Assume many of the services you use have had their data stolen at some point and if you re-use passwords, criminals get access to your whole life, not just one account.

Piano giveaway scams are strangely persistent. Here is one we received this month:

```
I am offering my late husband's Yamaha
Piano to anyone passionate about musical
instruments. Please inform me if you are
interested or if you know someone who
might appreciate this instrument.
```

The scam is to get you to pay for a moving company to send you the free piano. The web site they send you to is fake, and they usually request payment through a text message or cash app. The piano never comes and you have no recourse.

Boss gift card scams involve a text or email from someone claiming to be your boss. They often know some of the relevant names to make it convincing. They may say they are stuck in an important meeting or trapped at the airport and need you to purchase a gift card urgently so they can (schmooze a client, pay a fine, pay for an office party). They may include details about why they are using a different phone or email (phone battery dead, laptop stolen, etc.)

Any requests for secrecy (e.g. “the office party is a surprise”) or gift cards are big red flags. Gift cards are favored by scammers because they are nearly untraceable and easy to sell on the **dark web**.

In another boss scam that happened to a company we know, "The boss" emailed an accountant requesting a copy of all the employee W2 forms. The employee replied to the email and attached the 20+ PDF requested, happy to be doing the job efficiently, only later realizing the email address was not the boss's. They had just sent personal information on all of the employees to a criminal.

Invoice fraud scams have ramped up in recent years. People who work in any accounting or finance related department are most likely to receive these. They can be as simple as a request to pay a fictitious invoice, up to a longer term scam to change banking details in order to siphon thousands or millions of dollars.

A variant gaining popularity is a message that claims to be from a department head, forwarding an invoice from a vendor, imploring you to pay it quickly. The text from a recent one we received said, "Could you please process this Outstanding past-due invoice today? This is a new vendor." It preys on our desire to do a good job, to not be seen as inadequate (even by a stranger), in the hope we will rush the payment and only consider the details later.

Phishing and Spear Phishing scams involve tricking you into taking action or disclosing information that you shouldn't. Regular phishing is non-specific, such as a mass spam email with a link to a fake bank login page. The target is anyone willing to click that link. Spear phishing is focused on a particular person or role. The Boss gift card scams might be classified as spear phishing, especially if they include details about real people and companies.

A heinous phishing scam we learned about tricked a New Mexico company out of a lot of money. The target was a general contractor with a state contract. By using lookalike fake domains (think "willls-engr.com" instead of "willis-engr.com", with the 2nd "i" replaced with an ell-as-in-lima) they informed the Accounts Payable department about new bank name and routing number for ACH payments to their largest sub-contractor. They subsequently made a few very large payments for this project to the criminal's account before anybody realized there was a problem. The FBI got involved but only after the money had been moved, probably to an untrackable jurisdiction.

Another popular scam is a message from an employee to HR with new banking details for their paycheck direct deposits. We have received this one ourselves and could have fallen for it if we weren't already aware of this ploy.

Yet another common one is a fake receipt for some software (often Norton or McAfee). Of course you want to click the attachment to set them straight, but the attachment is malware.

Lessons and Advice

We hope that seeing these examples will help you recognize these scams and the many variants yet to be created. It is fantasy to expect technology to keep 100% of these out of our inboxes. It is up to us to exercise discrimination to protect ourselves, our loved ones, and our coworkers and employers.

Use these guidelines to avoid scams:

Gift cards and bitcoin - No legitimate transaction will ever be done with gift cards. Anyone demanding you pay in cryptocurrency, especially if it is for any kind of fine or past due bill, is up to no good.

Slow down - Urgency is the scammers number one tool to make you act without thinking. If there is even a spark of a thought that the request is not real, **stop**. Take a breath. Ask someone to look at it with you. Don't let them short-circuit your critical thinking.

Verify the source - We used to tell people, "Never click a link in an email". Unfortunately, it is hard to function in our society without occasionally clicking email links. But you can still protect yourself. **Never click a link in a message from your bank or any financial services company.** No matter how legitimate it looks, you don't have to click the link they give you to access it. Log in to the company's web site yourself and look up the information. If you can't find it, call the bank and ask.

> Remember that scammers can very easily send an email that includes all of the bank's branding and images.

Don't risk it, use your own bookmark to log in to the bank's site.

Verify the email - This is a special case of verifying the source. Email addresses have two parts, the "comment" and the "address". The comment part is usually in quotes and can say anything (the computers ignore it). The real address is in angle brackets. As in:

"SWCP Help Desk" <help@swcp.com>

Unfortunately many email programs **only** display the comment and not the address. If your email software only shows "SWCP Help Desk" for the above sender, they would show the same thing for this **bad sender**:

"SWCP Help Desk" <scammer@criminal.org>

This failing of software design is responsible for a great many scam victims. Usually, if you hover your mouse over the sender name it should show you the real email address. This will quickly reveal many scammers (such as the "employee" changing their bank details).

On a final note, many people are embarrassed when they get scammed, or are afraid of looking stupid when they ask questions to double-check something. You need not feel that way! Extremely experienced people steeped In scam knowledge can still get taken in. **Cory Doctorow tells how he fell victim just a few weeks ago in this essay**.

Stay safe!

Southwest Cyberport - swcp.com
New Mexico's Expert Internet Service Provider since 1994
505-232-7992 | Support: help@swcp.com
5021 Indian School NE, Ste. 600,
Albuquerque, NM 87110
Click on bold blue type in browser for links.