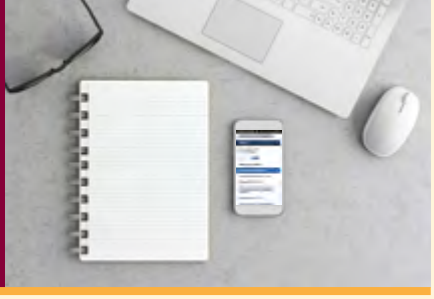

Attack of the Spoofers

By Anthony Hughs

Anthony Hughs is an award-winning technical writer. He has been working in computer science since 2000. His goal is to write articles that are easily digested by non-technical readers, while remaining scientifically sound for IT Professionals. In his free time, he enjoys the great outdoors.

While taking a moonlit walk in Napa, California, I found myself within earshot of two gentlemen standing near the road. They were talking about how they had been "hacked" on Facebook and how *nine of their friends had been hacked as well.* As I was strolling past them, I couldn't help but think about how often I've heard this very story. Seeing friends post "do not accept friend requests from so-and-so pretending to be me" is a semi-regular occurrence on social media. It struck me then how pervasive spoofing has become, as I had also recently witnessed an uptick in this behavior while on the job as a technical consultant for Kraft Kennedy. Upon closer inspection, I realized how often people confuse phishing, spoofing, and spear-phishing. Phishing has nothing to do with Ben & Jerry's ice cream, spear-phishing has nothing to do with diving in the ocean, and spoofing is a lot like it sounds.

If you ask around, you will be hard-pressed to find someone who doesn't at least know one person who has been "hacked" on Facebook, Instagram, LinkedIn, etc. We know that spoofing, or the practice of fraudulently imitating others online, exists. Yet we still find ourselves with the illusion of safety while at work or school. We feel protected by our IT department.

Most People Don't Know the Difference

According to the most basic explanation, spoofing is the method of delivery – a forgery of an email, website, or Facebook profile. Usually the spoof itself is very convincing. The spoof is not a person or an actual attack but rather a "magic show" that attempts to trick your eyes into believing it's all real. In staying true to the magic show analogy and for the purposes of this article, I will refer to these "magicians" as "Spoofers." I am choosing this term because you do not have to be a hacker to pull off a convincing email spoof and Spoofer has a nice ring to it.

One of the primary things a Spoofer will do when sending spoofed emails is change the "From" address on the email "envelope" so it appears to come from someone else. An analogy would be like sending a letter to someone through the postal service but changing the return address on the letter so it appears to come from someone else, or to reflect a new last name.

Phishing Is Less Personal Than Spear-Phishing

A successful phishing attempt will usually come in the form of a spoofed email from a corporate entity that asks you to go to a spoofed website and enter your username and password. This is impersonal as the only thing they might know is your name and email address. The same attempt might be made to thousands of other people simultaneously. The spoofed website will appear real to the untrained eye, largely dependent on the sophistication of the hacker. Entering your credentials gives them access to said account. In the blink of an eye, you are redirected to the real

website, none the wiser while they run off to the proverbial bank.

An All-Too-Real Threat

Spear-phishing is a personal, targeted ploy, devised to trick you, your coworkers, and those you love into giving up something extremely valuable. Spoofers take the time to construct an email, which appears to come from an associate of yours. Then they pretend to be the associate in order to leverage your trust. They always have a goal in mind, whether it's your privacy, your passwords, or your hard-earned cash. All the while, you believe you are actually conversing with *someone close to you*.

Recently, I've overseen multiple accounts of attorneys and law firm staff that were actively targeted by Spoofers. In these cases, the Spoofers seem to be getting better at email spoofing and closer to getting what they want – cold hard cash. For example, a law firm with about 75 people was recently the subject of a spear-phishing attempt. I'll call them Company X.

In the example of Company X, the email appeared *at first glance* to be from one internal employee to another. The subject line of the email read: "Financial Obligation." The body of the email was the *simple* request of "$11,986.90 USD due immediately." These are typical tactics that email Spoofers employ:

- An urgent subject line from a well-known associate
- Email signature appears legitimate
- Corporate logos in place
- From/Reply To: address is "spoofed"

Company X spares few expenses when it comes to technology. The firm actively protects itself with firewalls, anti-virus, email protection services, and by contracting a managed services provider for its IT needs. Spoofing, in contrast, can be done without fancy gadgetry. It entails bypassing IT security, no matter how big the budget allocated to it, through clever use of social engineering. The reason this works is because *it's not a virus or a direct hacking*; the risk is in the convincing nature of the ploy. From a security systems standpoint, the email appears legitimate. Spear-phishing is an example of why security awareness training is the most important aspect of a law firm's security program.

Let's Dissect a Spoof

How do you know if an email is legitimate or fake? In the previous example, the recipient of the fraudulent email rightly asked the IT department to check its legitimacy, stating that the address of the sender used the firm's defunct email suffix. She knew that the old email address had been retired some time ago, which made this seem especially odd. Still, she strongly considered sending the money before becoming suspicious. If it was an actual bill, of course she would have paid.

During my investigation, I reviewed the firm's email protection service (Mimecast) and confirmed that no one had sent an email to the recipient from inside the firm. Then, I took a closer look at the original email and found they had actually sent the message from Gmail. Once we knew for certain the email came from outside the firm, the spoof was averted. This is not to say that the Spoofer might not try to spear-phish this person again, but Company X is on higher alert now so it is less likely to happen.

No one wants to be the one who tells a hacker from the "dark web" that their publicly traded company is entering a merger, or be responsible for wiring large amounts of money to a fraudulent entity. However, with all the security measures our IT departments take, it's almost too easy to think we are impervious to attack. This is what makes spear-phishing effective. When it comes to spoofing, the human is the weakest link. Yes, that's right – you.

How to Defeat a Spoofer

Spoofers typically use several methods for trying to trick us into believing them, a few of which are described above. In the case of Company X, the hacker knew an email address currently in use and the name of its owner, as well as the name and email of someone no longer with the firm. Using this information, the Spoofer changed the envelope on the email to look like it was coming from the former employee's email address and sent the email. To build a compelling deception, Spoofers study you, your firm, your partners, etc.

If you receive an email from an entity requesting money, passwords or personally identifiable information, you should pause. Take a moment to consider if the message is real. Above all else, if the request is strange and "out of the blue" you should ask your IT department to review. If you can't do that (and you can't call the sender on the phone) you should compose a new email. That is, do not reply to the strange email. Composing a new email will use the email address already stored in Outlook, on your phone, in Gmail, etc. and is more likely to go to the correct recipient. If you reply to the spoofed email, your message will be routed to the attacker instead of who they are pretending to be. Whatever you do, you should not engage in a prolonged conversation with the Spoofers. This is akin to a fisherman feeling a tug on the line.

How Can You Protect Yourself

Protecting yourself during your personal time does help protect the firm. One way to do this is through the use of two-factor security on Facebook, Instagram, and LinkedIn. Enabling this adds an extra layer of security because it requires access to your cell phone or email account in order to access your social media accounts.[1]

When it comes to phishing, spoofing, and spear-phishing it is our awareness and ability to step back that is most effective against the attack of the Spoofers! ■

1. LinkedIn Two Factor, https://www.linkedin.com/help/linkedin/answer/544/turning-two-step-verification-on-and-off?lang=en; Facebook Two Factor, https://www.facebook.com/help/148233965247823; Instagram Two Factor, https://help.instagram.com/566810106808145?helpref=search&sr=1&query=two%20factor.