Is That Email Attachment Malware in Disguise? How to Protect Yourself From a Spear Phishing Scam

By Gary Davis on Apr 25, 2017

The term phishing is floating all over the news these days. And no, I'm not misspelling the fun sport where you try to reel in some seafood for dinner. I mean the type of cyberattack that uses social engineering, aka manipulation, online to trick someone into giving up their personal data. Some of the most recent and powerful examples of a spear phishing attack are the Shamoon2 attacks we've seen in Saudi Arabia, which infected machines with malware and destroyed systems through a specific type of phishing called spear phishing.

So, how did this specific spear phishing attack work, exactly? Cybercriminals targeted specific organizations in Saudi Arabia with emails that included malicious attachments in them. Then, when victims clicked and opened the attachment, they were infected, valuable company data was taken and systems were quickly wiped.

Spear phishing has been around for quite some time, but has been as effective as ever lately. Spear phishing's success is based in familiarity. Usually, cybercriminals pretend to be an organization or individual that you know, and include a piece of content—a link, an email attachment, etc.—that they know you'll want to interact with. For example, cybercriminals have taken advantage of tragedies in the headlines, and used targeted emails claiming to be a charitable organization asking for donations. In the case of Shamoon2, the attackers lured in victims with a tempting email attachment sent from organizations the victims were likely to trust. But instead of giving to their charity of choice, or opening a seemingly harmless workplace attachment, victims then self-infect their systems with malware.

Moral of the story: spear phishing (and regular phishing) attacks can be tricky. However, fear not, there's a lot you can do to stay on top of this threat, as well as protect your inbox and, therefore, your personal data, from attack. For starters:

-Go straight to the source. Spear phishing attacks can be easily deceiving. In fact, cybercriminals have been able to impersonate known, credible charities or an employer's business partners and customers. So, if you receive an email from an organization asking for donations or a partner asking you to open a file you didn't request, a good rule of thumb is to go directly to the organization through a communications channel other than email. Go to the company's site and do more research from there. That way, you can ensure you're gaining accurate information and can interact with the right people, rather than cyber-attackers.

-Always check for legitimacy first. Spear phishing emails rely on you—they want you to click a link, or open an attachment. But before you do anything, you always need to check an email's content for legitimacy. Hover over a link and see if it's going to a reliable URL. Or, if you're unsure about an email's content or the source it came from, do a quick google search and look for other instances of this campaign, and what those instances could tell you about the email's legitimacy.