# How to protect yourself from 'spear phishing' hacking technique

19 July 2018, by Christian Hetrick, The Philadelphia Inquirer

Credit: CC0 Public Domain

As sophisticated as the scheme was by Russian intelligence agents to interfere in the 2016 presidential election, they used a simple hacking technique, among others, to infiltrate the email accounts of Democratic operatives, according to Special Counsel Robert Mueller's latest indictment. And that technique—known as "spear phishing—remains a threat not just to campaign officials but to employees and consumers.

Spear phishing is a scam in which cyber criminals pose as trusted sources and send phony electronic messages to targeted individuals to trick them into revealing sensitive information.

In the case of John Podesta, the chairman of Hillary Clinton's presidential campaign, it was a misleading email that looked like a security notification from Google, asking Podesta to change his password by clicking an embedded link, according to the indictment filed Friday. Podesta followed the email's instructions, changing his password and giving hackers access to 50,000 of his emails.

But spear fishing could come in the form of an email that appears to come from your boss, asking you to send your W2 form. Or a message with an expected invoice, requesting that you wire the money to an account controlled by bad actors.

"The indictment really illustrates the many uses this technology can be put," said Edward McAndrew, a former federal cybercrime prosecutor and co-leader of Ballard Spahr's privacy and data security group in Philadelphia. "It's not just about stealing someone's personal information. It's about financial fraud, or in this instance, even election fraud."

**How it's done**

In typical phishing scams, cybercriminals send blanket emails to a large swath of users, hoping someone will take the bait and download an infected attachment or click a link to a phony website.

Spear phishing scams, by contrast, are tailored to specific targets. Hackers will research an individual ahead of time, scanning social media accounts and public information to learn a person's job, friends or interests to craft a trustworthy email.

"They'll figure out where you work and who your colleagues are and try to send a fake email that looks like it's from one of your colleagues," said Gabriel Weinberg, CEO and founder of Paoli-based DuckDuckGo, an internet search engine that doesn't track or store user data.

That's what happened Tuesday at Weinberg's company. One of his employees received an email from a sender using Weinberg's name asking, "I need you to help run a task. Let me know if you're unoccupied," according to a copy of the message. The sender posing as Weinberg wanted to "gift out some Apple Gift Cards to some clients." Weinberg

and his colleague didn't bite.

The person pretending to be Weinberg used an email address that wasn't even close to resembling the real thing. But Michael Levy, the chief of computer crimes for the U.S. Attorney's Office in Philadelphia, said cyber criminals will typically create email addresses that are nearly identical to those of trusted sources, sneaking in an extra letter or using a zero instead of a capital "O," for example.

In some cases, such as the Russian hack of the Democratic Congressional Campaign Committee, spear phishing emails will direct users to phony websites, where victims will enter their credentials and unwittingly give hackers their usernames and passwords. In the DCCC case, Russian agents then installed malware on at least 10 of the committee's computers, according to the indictment, allowing them to monitor individual employees' computer activity, steal passwords and maintain access to the DCCC network.

"There are two ways to get into computers," Levy said. "There is the sophisticated hacking where you figure out how to break through a security system ... [or] you attack the weakest link in the security system, and that's the user."

Once hackers have access to a company's email system, "they will sit and watch to learn as much as they can about people," Levy said, adding that cyber criminals can glean anything from employees' email habits to the name of the company president's wife.

McAndrew, of Ballard Spahr, said once hackers gain entry to an email account, they can peruse a user's messages, work calendars and contacts, as if someone is "virtually looking over their shoulders."

"You're able to know about events before they happen by reading about them," McAndrew said. "You know what's coming up."

Hackers aware of an upcoming payment can pounce by sending spear phishing emails to trick recipients into wiring money to accounts under the hackers' control, McAndrew said.

Victims of internet crimes suffered more than $1.4 billion in losses in 2017, almost doubling since 2013, according to an FBI report on the issue released in May. Crimes listed as "business email compromise/email account compromise" accounted for more than $676 million of that 2017 total, representing the largest category of loss.

**How to protect yourself**

One way to reduce the risk from spear phishing is use multi-factor authentication, which adds an extra layer of security by requiring not just a username and password, but knowledge or possession of something that only that user has, such as a code sent to a cell phone.

"Even if you get tricked and you go to some bogus site and type in your password, it will be useless without" the other piece of information, said Anthony Vance, director of Temple University's Center for Cybersecurity.

Vance suggested using twofactorauth.org, which tells users whether websites support multi-factor authentication. Major services such as Google or Yahoo allow users to activate the service.

Experts said individuals should use some common sense too. Resist the urge to click links or attachments from an unknown source or unexpected message. Check with colleagues before responding to a suspicious email.

"The number one thing people can do is scrutinize every single email they receive," McAndrew said.

APA citation: How to protect yourself from 'spear phishing' hacking technique (2018, July 19) retrieved 25 May 2019 from https://phys.org/news/2018-07-spear-phishing-hacking-technique.html