
SPEAR PHISHING 101
sendio®

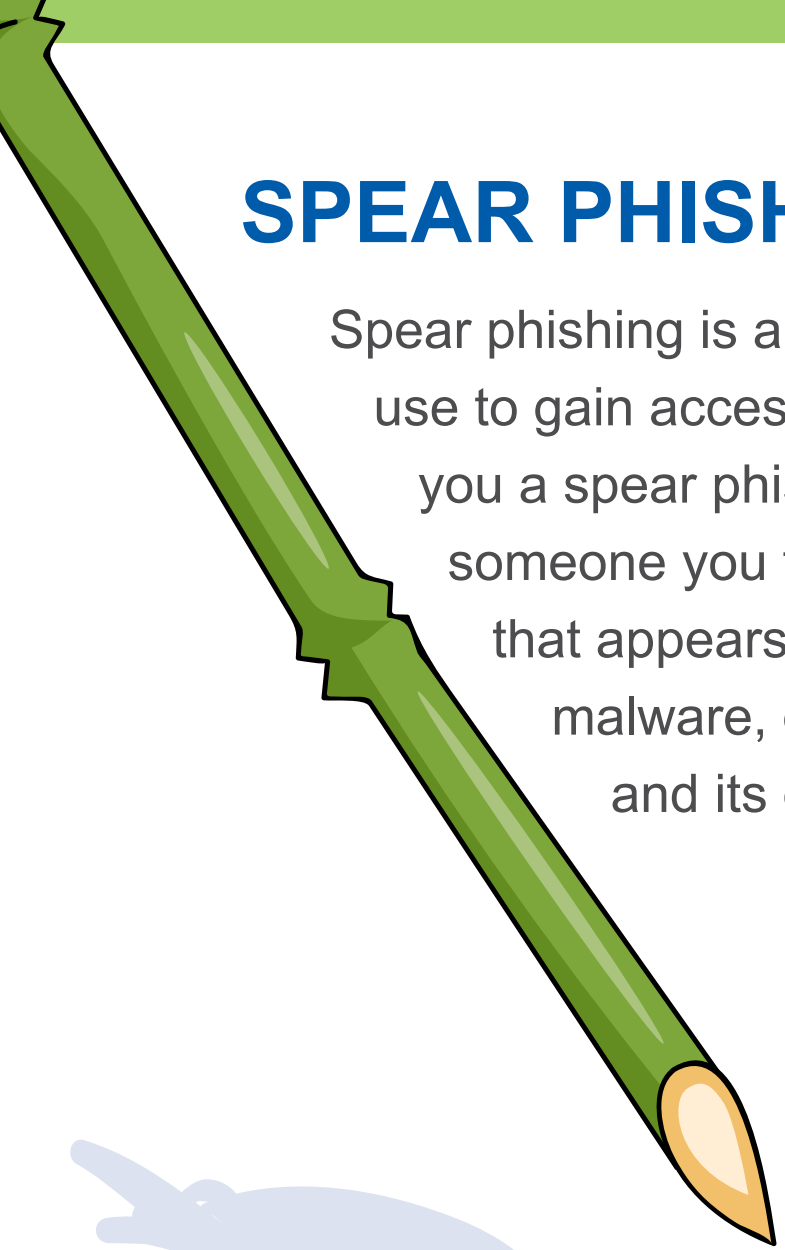
IT'S THIS EASY...

At 6:15am one morning this past February a Forbes senior executive woke up and checked her email to find an unread message that seemed to come from a Vice Media reporter asking her to comment on a Reuters story that was linked in the email. After clicking the link, she was prompted to log into her email again. After providing her log-in credentials, she was taken to a blank page. She didn't think much of it, and then continued with her day without knowing she had just sent her email credentials to a hacker.

The senior executive's email account was used to send another fraudulent email to Forbes staffers. At 7:45am that same morning, a Forbes staffer received the email that asked him to check out a news story that was recently posted about Forbes. The staffer—a "super–administrator" on the Forbes website—entered his email credentials into a fake but identical looking webmail log–in page. After he hit "submit" to log–in, he was forwarded to an old NBC News story, and it hit him: **He had been spear phished**.

Just like that, Forbes lost control of its website for over 24 hours. The Syrian Electronic Army announced on its Twitter feed that it had hacked Forbes. It later wrote that it had gained access to the million-user database, and asked for bids from possible buyers before declaring that it would release the hacked usernames, emails and hashed passwords for free. Soon after, it published the database for all the world to see.

SPEAR PHISHING—WHAT IS IT?



Spear phishing is a specific kind of email phishing attack hackers use to gain access to sensitive data. When someone sends you a spear phishing email, it looks like it's coming from someone you trust. The email contains a link to a website that appears to be legitimate, but the link delivers malware, giving the hacker access to your network and its data.

HOW IT'S DIFFERENT

Normal phishing emails are typically sent out to huge lists of people. They cast a wide net with the hope of catching a few fish. They are often easy to spot; their hallmarks are:

- Misspellings
- Poor grammar
- Tacky subject lines
- Odd Formatting

From searchsecurity.techtarget.com:

In the case of spear phishing, however, the apparent source of the e-mail is likely to be an individual within the recipient's own company and generally someone in a position of authority. Visiting West Point teacher and National Security Agency expert Aaron Ferguson calls it the "colonel effect." To illustrate his point, Ferguson sent out a message to 500 cadets asking them to click a link to verify grades. Ferguson's message appeared to come from a Colonel Robert Melville of West Point. ***Over 80% of recipients clicked the link in the message.*** *In response, they received a notification that they'd been duped and warning that their behavior could have resulted in downloads of spyware, Trojan horses and/or other malware.*

The precise nature of spear phishing makes it extremely difficult for your email security provider to identify the attack and prevent it.

WHY IT MATTERS

All it takes is you clicking on one link in a spear phishing email for a hacker to gain access to valuable data like credit card information, trade secrets, or social security numbers; it all depends on what the hacker is looking for. If your email security system isn't designed to stop spear phishing in its tracks, you are vulnerable to these kinds of attacks.

Let's take a look at some notable spear phishing attacks from the past year...

TARGET

Hackers used a spear phishing email to gain access to **110 million Target shoppers' credit card data**. All it took was an employee at an HVAC vendor that does work for Target clicking a link in a spear phishing email.

Forbes estimates the hack cost financial institutions more than $200 million and cost Target around $148 million. That adds up to more than $350 million in damage done by a spear phishing attack.

CHINESE HACKERS

The FBI has named five Chinese military officials to the Most Wanted list for their **hacking of U.S. metals and solar power companies**.

Chinese hackers use spear phishing attacks to steal trade secrets of companies around the world—and especially in the U.S. Although it can be difficult to put a number on the value of innovation lost through these attacks, some estimate it may be as much as $5 trillion dollars each year.

ASSOCIATED PRESS

Members of the Syrian Electronic Army—a group loyal to Syrian president Bashar al-Asaad—used a spear phishing email to gain **access to the Associated Press Twitter account**.

Once they had access, they published a false tweet claiming President Obama had been shot. The tweet caused a $136 billion drop in the stock market.

SENDIO COMPLETELY ELIMINATES THE RISK OF SPEAR PHISHING ATTACKS.

Sendio's Email Security Gateway™ stops spear phishing emails in their tracks. The Email Security Gateway is a multi-layer defense against malicious emails and spam.

Here's how it stops spear phishing before it makes it to an inbox:

Sender Policy Framework:

The SPF—sender policy framework—check employed by Sendio prevents spoofing by confirming that the sending IP address is officially referenced in the sending domain's SPF record. If the SPF check fails, the email is held on Sendio and not delivered to the user's inbox.

Smart Whitelisting:

Unlike other email security providers that don't scan emails from addresses on your whitelist, Sendio scans every email to prevent you from falling prey to spear phishing.

SENDIO IS DIFFERENT.

Most email security providers use an SPF check, but if an email sender is on your whitelist, emails from that person go straight to your inbox without being scanned for spoofing. Sendio scans every email, every time to keep your network safe.

About Sendio: Sendio offers solutions to enterprises and institutions that will increase employee productivity while eliminating spam and malicious emails. To learn how Sendio can help keep your organization safe from spear phishing, call (877) 363-2772.

Sources:
http://www.forbes.com/sites/andygreenberg/2014/02/20/how-the-syrian-electronic-army-hacked-us-a-detailed-timeline/
http://www.huffingtonpost.com/2014/02/12/target-hack_n_4775640.html
http://blogs.wsj.com/corporate-intelligence/2014/08/05/an-expensive-hack-attack-targets-148-million-breach/?KEYWORDS=%22credit+cards%22
http://time.com/106319/heres-what-chinese-hackers-actually-stole-from-u-s-companies/
http://www.theepochtimes.com/n3/326002-the-staggering-cost-of-economic-espionage-against-the-us/
http://www.washingtonpost.com/blogs/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/