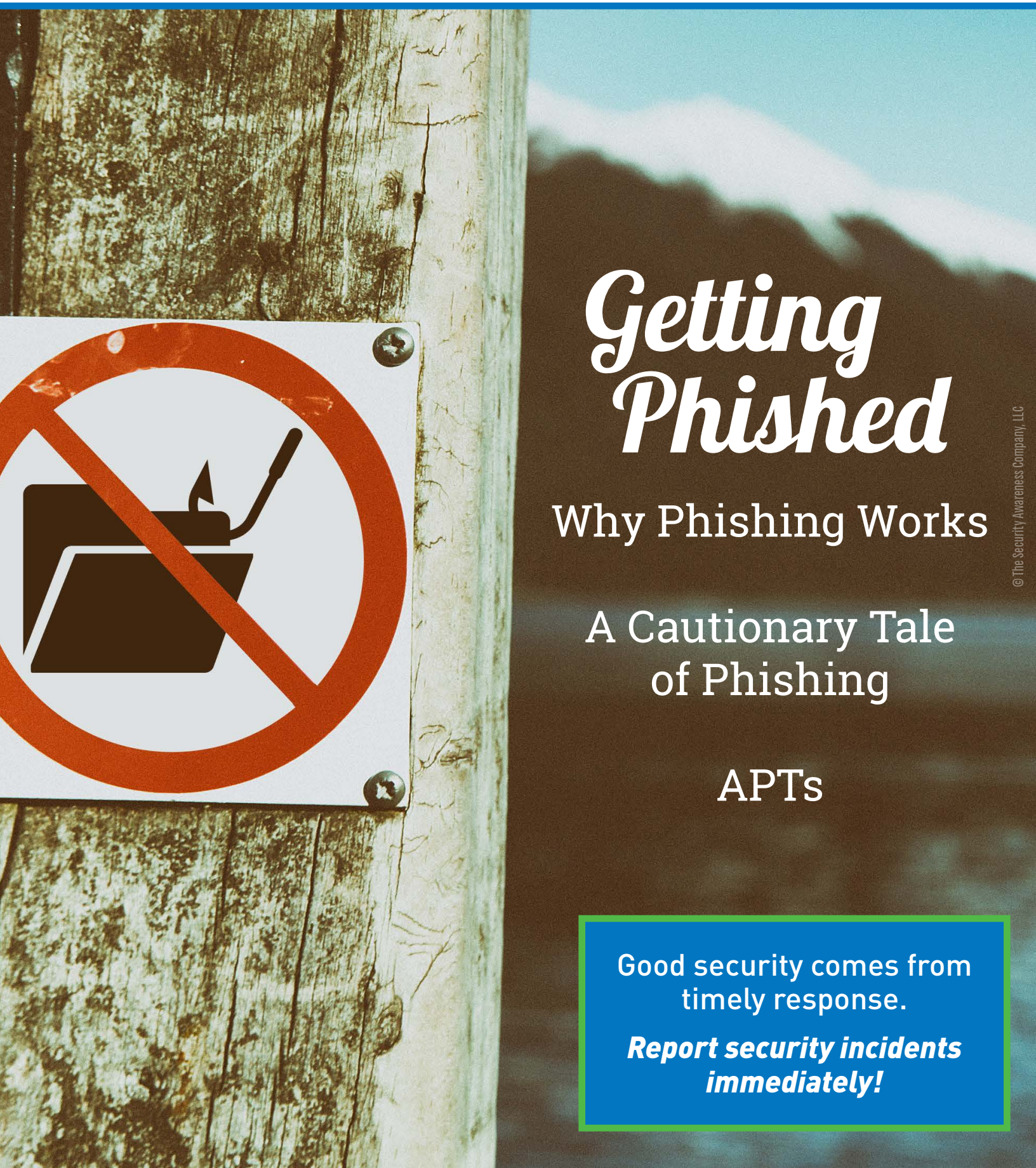
Northfield Bank

Information Security Advisor

December 2018



Getting Phished

Why Phishing Works

A Cautionary Tale of Phishing

APTs

Good security comes from timely response.

Report security incidents immediately!

Why Phishing Works

A successful phishing attack accomplishes two basic goals: ***it gains the trust of victims and exploits their emotions.*** Take, for example, those classic advance-fee scams that promise a large sum of money for a small up front payment. You would never fall for one of those, right? Of course not. They're incredibly easy to spot, thanks to their too-good-to-be-true nature. But other phishing scams are more advanced.

Imagine a friend of yours is looking for a job. She posts her resume on various sites and sends out applications. Then, she finally receives an email, that appears to come from Linkedin, with a great job offer. ***All your friend has to do is click the link and upload her personal details. But is it a scam?*** More importantly, would your friend, who has been on the job hunt for several months, even question its authenticity?

Now let's flip roles. Let's say you handle the hiring of new employees and you get lots of emails from applicants with attachments. ***How difficult would it be for a social engineer to push a malicious attachment, disguised as a resumé, to your inbox?***

What about emails that appear to come from someone you know? Let's say a friend sends you a message that he's traveling abroad, has been robbed, and urgently needs *you* to wire him money in order to buy a ticket home. How would you respond?

It is easy for social engineers to leverage emotions like compassion or concern against their targets. It gets even easier when their targets are at a point of desperation, often related to financial need.

Simply put, people fall for advance-fee scams. People fall for fake job offerings. People fall for threats that claim to come from tax collection agencies. ***Trust, desperation, and fear: the most effective weapons of scammers.***

Phishing Identification Checklist

- ☐ Does the email contain poor spelling and/or bad grammar?
- ☐ Is the email awkwardly worded or nonsensical?
- ☐ Is the "from" address unrecognizable or just plain weird?
- ☐ Does the email promise large sums of money or other unbelievable offers?
- ☐ Does the email use threatening language?
- ☐ Does the email contain a sense of urgency?
- ☐ Does the email have a call-to-action such as clicking a link?
- ☐ Does the email contain an unexpected attachment or request for money?

If you had to check any of these boxes, beware! You could be under attack!

As always, follow our organization's policies and report security incidents, such as potential phishing attacks, immediately. If you have any questions, please ask!

DID YOU KNOW...

Email addresses can be spoofed, or forged, to make messages appear to come from legitimate sources. Victims are much more likely to cooperate when they believe they are communicating with someone they know, which is even more reason to fully scrutinize all requests for sensitive info or money!

A Cautionary Tale in Phishing

The following account from a colleague details how easy it is to get phished. As you read it, just think about your day-to-day routine and ask yourself: would this ever happen to me?

I probably get about 150 emails a day. Sometimes more. If I were to guess, I'd say at least two or three of those are spam or phishing of some sort. Needless to say, I'm pretty good at spotting them.

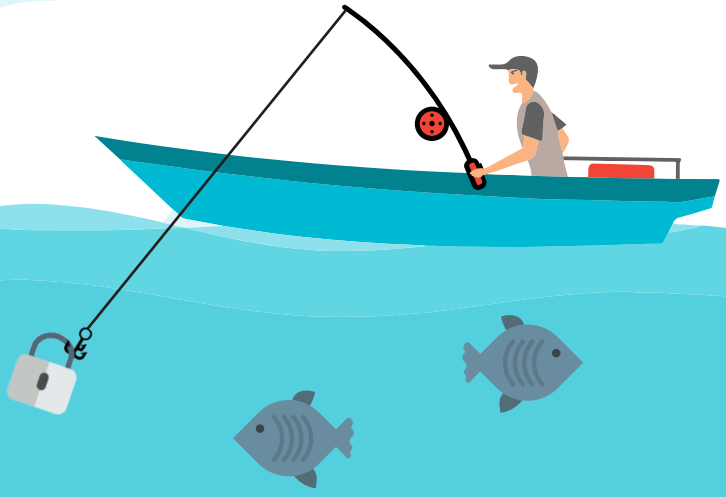
At least I thought I was.

It was one of those weeks when the perfect storm hit. We onboarded several new employees, plus added a few major client accounts. All good things, but incredibly busy. Just lots of paperwork.

So, late Friday afternoon after a long week, I was processing tax info for my new co-workers. Maybe I was working too fast, not being thorough enough. Hard to say. But I only had a few more to get through. I opened an email that I thought was from a new employee and downloaded the attached document—standard stuff.

But when I opened the document, it was blank. Confused, I went back to my email client to see if maybe it had messed up during the download. But before I could even get there, my antivirus suddenly popped up in the middle of the screen with an alert that it had detected a hostile threat. Five seconds later, my whole screen went black and was replaced by a **ransomware** note.

This victim's story illustrates an important lesson in cybersecurity: anyone can make a mistake, even the most cautious person. Busy work seasons and long weeks can lead to security awareness being a bit lax. But remember that all your hard work will be for naught if our networks are compromised by a phishing attack! Slow down, stay alert, and think before you click.



Ransomware Everywhere

According to a recent study, ransomware attacks have surged, with over 181 million attacks in the first six months of this year. For reference, that's a **229% increase** over the same time frame in 2017. Why does this matter to you? Because it shows that phishers have changed their bait. For years, their goal was to infect systems with malware and steal sensitive data. That still happens, but the market for selling sensitive data on the dark web has become oversaturated, thanks to multiple major data breaches.

Hence, scammers have adopted ransomware, which promises a much easier and quicker way to profit. Keep that in mind as you go about your daily routines. **One wrong click** could lock up our entire network!

High-Profile Ransomware Case

Early on a Thursday morning in March 2018, the City of Atlanta came under attack. A ransomware variant known as SamSam shut down five of the city's 13 local government departments, crippling their systems and knocking nearly a third of their programs offline. As hours and days passed, the attack prevented the city from collecting revenue. It left residents unable to pay utility bills or request services. It forced the police and other city departments to file paper reports, grinding operations to a halt.

In the end, the city's systems were offline for over a week, 6 million people were impacted, and the cost of recovery is expected to reach nearly nine million dollars.

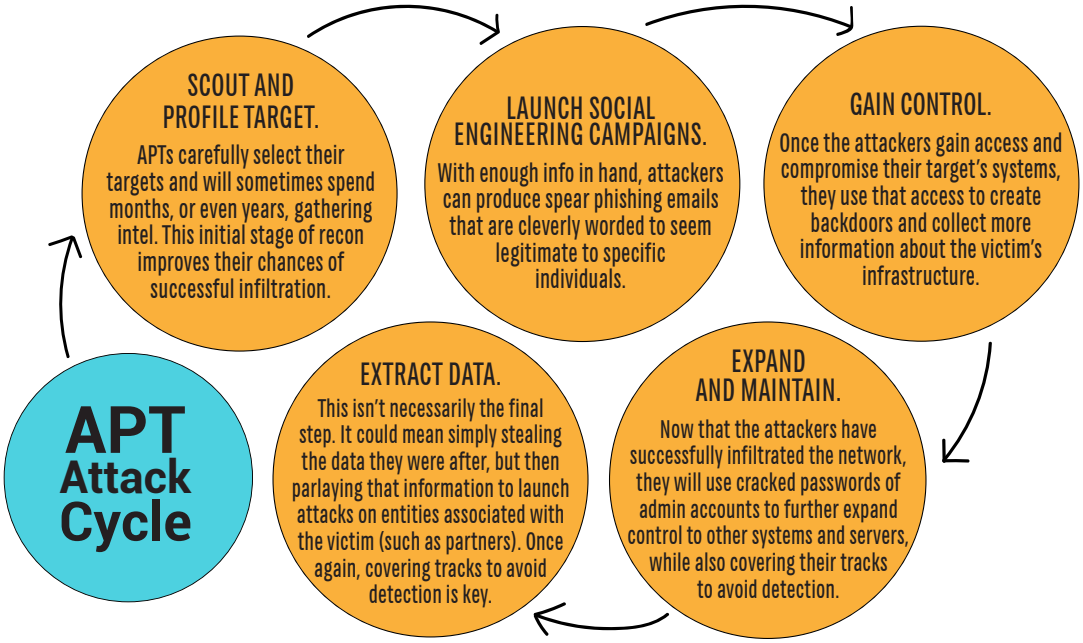
This attack exemplifies the dangers of ransomware. And even though SamSam doesn't necessarily rely on phishing emails to infect systems *(it utilizes weak and stolen credentials to gain access to vulnerable servers)*, most other variants do, and their impacts present just as much of a threat. Once again, use common sense, slow down a bit, and think before you click!

APTs

APT (Advanced Persistent Threats)

Definition: advanced cyber-attacks that are carried out by well-funded entities which target specific organizations and other entities.

Is there a more intimidating combination of words than Advanced Persistent Threats? Certainly not in the world of information security. As the name suggests, APTs use advanced tactics to infiltrate and compromise their targets. Unlike typical, generic phishing campaigns and other attacks, APTs aren't random. If you're under attack, you have been targeted with purpose.



PREVENTING APTS FOR MANAGEMENT AND IT

GUARD YOUR PERSONAL INFO · Remember that when it comes to social media, less is more! This step is especially important for management and upper-level employees with high-level access to systems and networks. Never publicly post any info that could be used against you, and by extension, our organization.

PERFORM A RISK ASSESSMENT · Every employee and organization should know which information they can access, as well as its relative value to cybercriminals. By identifying your most valuable assets, you can then develop a strategy to protect them.

TEST YOUR DEFENSES · How good are your firewalls, both digital and human? Are you confident that your employees will spot phishing attacks? How strong is your physical security? To answer these questions, security experts recommend hiring penetration testers to launch simulated attacks against your organization. These attacks can find potential weaknesses *before* the attackers do.

KEEP SYSTEMS UP TO DATE · An unpatched, out-of-date system is an APT's best friend. No excuses: leaving your systems unpatched invites risk and, eventually, data breaches.

ROUTINELY AUDIT ACCESS CONTROLS · Do you know which employees have access to which parts of your networks and data? Does anyone have more access than what's necessary for them to perform their job functions? Properly assigned access controls can help prevent an attack from spreading.

TRAIN YOUR EMPLOYEES · Security awareness training needs to be thorough, but also personal. This means you should do your best to develop a program to which your employees can relate. The more they understand how data breaches and other attacks could impact them from a *personal* standpoint, the more likely they will be to absorb and act upon the information you provide.

PREVENTING APTS FOR END-USERS

RESPECT PRIVILEGED ACCESS.

No matter what your responsibilities are within our organization, always respect the access you've been granted. Never allow someone else to use your credentials for any reason.

THINK BEFORE YOU CLICK.

The unfortunate reality of cyber threats is that we're only a click away from our data falling into the wrong hands. Stay alert and use common sense!

REPORT SECURITY INCIDENTS IMMEDIATELY.

The classic "If you see something, say something!" applies to every element of our organization's security. From phishing emails to unknown persons, if you see something out of the ordinary, please report it ASAP.

ALWAYS FOLLOW POLICY.

Failure to follow policy, whether accidentally or intentionally, weakens our organization's security posture and puts us at risk. From the front desk to upper management, no one is above the policies we have in place.

WHEN IN DOUBT, ASK!

There are no useless questions when it comes to the security of our organization. If you want more information about a particular topic, or if you simply don't understand a specific policy, please ask!