INVESTMENT COMPANY INSTITUTE®
ICI Global
WASHINGTON, DC • BRUSSELS • LONDON • WWW.ICI.ORG

ICI VIEWPOINTS

AUGUST 23, 2016

# Cybersecurity at Work: The Risks of Information Sharing

By Peter Salmon

*Part of a series of* ICI Viewpoints *covering cybersecurity issues.*

In the last installment of this series, we wrote about the importance of information sharing. Though important, there is a balance to be struck; you don't want to share *too* much information. Growing up in New York City, for example, my friends and I would poke fun at drivers with personalized license plates. "Why would anyone want everyone to know where they were all the time?" was our usual comment.

Today, social media platforms are personalized license plates on performance-enhancing drugs. These platforms tell the world who you are, where you work, where you live, where you vacation and with whom, and perhaps even what you had for lunch. The information you share on these platforms makes it quite easy for cyber criminals to perform reconnaissance on you and your firm.

## Don't Get Hooked

"Phishing" is an attempt by criminals to obtain sensitive information by masquerading as a trustworthy source. According to the2016 Verizon Data Breach Investigations Report (VDBIR), 30 percent of all phishing emails are opened by recipients. Though some phishing emails can look legitimate at first glance, many are produced on an industrial scale and contain obvious errors when one takes the time to scrutinize the contents.

Spear phishing—an malicious electronic communication targeting a specific individual—is a tailored attack that leverages information specific to you. These attackers conduct reconnaissance exercises on their target victims—and perhaps the best place to gather valuable personal information is from social media posts.

Let's say, for example, that a system administrator at your firm describes his job on his favorite social platform, providing critical screening information and incentive for an attacker to dig deeper. By scanning other social networking sites, the attacker likely can get his email address, list of friends, travel schedule, etc.—information that will help the attacker craft a spear phish customized for him. (If you don't think an attack like this could be effective, keep in mind that the VDBIR states that 13 percent of those who opened a phishing email clicked on the attachment or link in the email, generally within four minutes of receipt.)

Though spear phishing attacks can lead to malicious websites full of malware, attackers (including those from nation states, hacktivist organizations, organized crime, etc.) often are looking to obtain credentials so they can attempt to bypass a company's information security defenses, rather than trying to break through an otherwise well protected network.

## Common Sense and Corporate Policies

The nature of such attacks means that, ultimately, users are the last line of defense. Antivirus signatures and firewalls will not necessarily prevent an otherwise legitimate-looking email from appearing in an employee's inbox. A critical eye and some good old fashioned common sense will go a long way in keeping firms from being affected by, and having to respond to, an attack.

So, how do you regulate information sharing? A corporate policy can help provide awareness of exposure and some basic standards. There are other prudent measures that firms and individuals might consider. On a personal level, one option is to remove or refrain from building a social media profile at all. Despite what your friends may tell you, it isn't the end of the world. You will be much less visible online, which makes collecting and combining valuable personal information more challenging for the attacker.

One variable that can help you make this decision is whether your position at your employer increases your attractiveness to attackers. Put yourself in the mindset of the attacker: who and what would you look for? Information on the social media profiles of senior executives, system administrators, or finance department staff might provide just what attackers want. Now, look at your online profiles: can an attacker easily find your employer's name, your job title, your email address, a list of friends, or their email addresses? Did you post something to a friend's page that reveals too much information, given this new perspective? At a minimum, if you do want a web presence, be thoughtful about what information you decide to share with the world.

Do you really need that online "license plate" that screams "look at me"? The consequences of not being thoughtful about your social media presence are real: they include the loss of sensitive personal information, damage to your employer's brand, disruption of business operations, and even significant financial loss. A good place to read about the potential effects of phishing is the SANS Securing the Human website.

Do you know how to pack for a trip? The next post in this series will examine this question and why it matters.

## Additional Resources

Information Security Resource Center

## Other Posts in This Series:

- Cybersecurity at Work: Creating Passwords That Are More Secure
- Cybersecurity at Work: Incident Response Plans and What They Entail
- Cybersecurity at Work: Exercise Is Important
- Cybersecurity at Work: The Benefits of Information Sharing Networks
- Cybersecurity at Work: The Risks of Information Sharing
- Cybersecurity at Work: Keeping Secure When Away from the Office
- Cybersecurity at Work: I Know What You Know!
- Cybersecurity at Work: To Confront Evolving Threats, Flexibility Is Key

Peter Salmon is ICI's senior director of operations and technology.

---