It seems that just like in old times (in cyberspace that means last year) the existence of “snake-oil” salesmen on the Internet is getting worse, not better. Rather than selling something medicinal or at the very least useful, these snake-oil salesmen of today have one intent only: to steal your personal information or worse, to distribute malware to your computer. One recent report issued by Symantec in April 2015 literally details scores of scams all designed to steal information and potentially ruin your computer (and others’ as well) and steal your personal information. We detail them not out of morbid curiosity of the utter gall of the snake-oil salesmen, but to hopefully inform and prevent the inadvertent “click on the link” circumstances which you and your company would rather avoid. We also point to other recently issued reports noting that other scams like phishing and spear phishing continue to be a bothersome and dangerous component of company emails. At the end of the day, as we discussed in our last article, continuous employee training and awareness of these sorts of scams is truly a strong part of the Holy Grail of Cybersecurity, along with certain network hardware components that can help stop “bad” emails before they get to your employees’ desktops.

Social Media Scams

“Where attacks of yesteryear might have involved a foreign prince and promises of riches through shady exchanges of currency, … today’s phishers scan social media for birthdays, job titles and anything else that can be used to create the appearance an email request is coming from a legitimate source.” As the Symantec Report points out, a lot of these email scams and offers are now generated through the explosive growth of social media sites such as Facebook, Twitter, and Pinterest. Here are some of them:

- **Manual Sharing** – These rely on victims to actually do the work of sharing the scam by presenting them with intriguing videos, fake offers, or messages that they can then share with their friends;

- **Fake Offerings** – These scams invite social network users to join fake events or groups with incentives such as free gift cards. Joining often requires the users to share credentials with the attacker or send a text message to a premium rate number;

- **Likejacking** – Using fake “Like” buttons, attackers trick users into clicking website buttons that install malware and may post updates on a user’s newsfeed, thereby spreading the attack;
Fake Applications – Users are invited to subscribe to an application that appears to be integrated for use with a social network, but is not as described and may be used to steal credentials or harvest other personal data; and

Affiliate programs – When you click on the link, these might allow you to get a free smartphone, airline ticket, or gift card. Caveat emptor: Nothing in life is free, especially when malware is attached thereto.

Phishing Attacks – Email Scams – Email Hijacking

We have talked in the past about the prevalence of phishing or spear phishing attacks against U.S. public companies. As noted in the recently issued 2015 Verizon Data Breach Investigation Report:  

Social engineering has a long and rich tradition outside of computer/network security, and the act of tricking an end user via e-mail has been around since AOL installation CDs were in vogue...

The first “phishing” campaigns typically involved an e-mail that appeared to be coming from a bank convincing users they needed to change their passwords or provide some piece of information, like, NOW. A fake web page and users’ willingness to fix the nonexistent problem led to account takeovers and fraudulent transactions.

Phishing campaigns have evolved in recent years to incorporate installation of malware as the second stage of the attack. Lessons not learned from the silly pranks of yesteryear and the all-but-mandatory requirement to have e-mail services open for all users has made phishing a favorite tactic of state-sponsored threat actors and criminal organizations, all with the intent to gain an initial foothold into a network.

Some of the statistics set forth in the Verizon Report are cause for concern:

- 23% of recipients now open phishing messages and 11% click on the links;
- 50% of the recipients open emails and click on the links within the first hour;
- The median time to first click on the link: one minute, 22 seconds!!

How Do You Stop Malicious Social Media/Spear Phishing/Email Campaigns

Obviously there are no good answers to these questions, especially in an era when the bad guys are sending such socially engineered emails that they look like they could come from your husband, wife, son, or daughter. They are that good. But here are some points to consider:

1. Anti-phishing training: As we noted in our previous article, many argue that the weakest link in cybersecurity is the person who is sitting in the chair in front of his or her computer. As such, we strongly advocate a consistent training program, as provided by various organizations, which can provide tailored solutions to your employee base, or specific sections of your employee base (like your IT department or your finance department), to help them change their behavior and discern between “good” emails and potential “really, really bad” emails which may contain malware packages just waiting to go off when someone opens the email or clicks on the link. Choose a program which can provide metrics and reports to either your compliance or IT security department, which might point out areas of risk such as divisions, departments, or employees who need further training.

2. Increase user training and advise workers on safe practices when using Facebook, Twitter, Snapchat, and other online services: Simply put, there are bad actors out there who will attempt to lure your employees into doing things or sharing information which may, at its core, contain or share malicious code with others. Adopt policies and procedures to educate your employees on social media website scams, which may include limiting use of such sites to their own devices. “It is key that all staff receive
security awareness training covering your acceptable usage policy for social networking. Promoting good practice and improving user behavior are the best methods of reducing the risks from this form of communication.”

3. **Employ DMarc Based Technology:** Many companies have chosen to employ a technology-based solution founded on DMarc, or “Domain-based Message Authentication, Reporting & Conformance.” DMarc is an Internet protocol specification that … provides visibility into email flows, and can tell receiving servers to delete spoofed messages immediately upon receipt, thus ensuring that only legitimate emails are delivered to inboxes.” DMarc allows companies to “pre-qualify” email providers who are “approved” to send your employees emails from those who may be attempting to spoof or clone domain names to send your employees malicious emails.

4. **Sandboxing:** Deploy a solution that checks the safety of an emailed link when a user clicks on it. The hardware solution that is employed examines the link-driven email and analyzes it against known malicious email threats and URLs and then “quarantines” them using anti-spam and anti-virus threat engines to see if those emails exhibit “bad” characteristics. These solutions can be used both “on premises” and if your email is handled by cloud mailboxes. It is better to check and stop the email before it gets to an employee’s desk where it could be inadvertently opened and spread malware to your network. Beware that not all sandboxing technology works the same, and it may not be 100% effective against all threat vectors, especially as bad actors get more and more sophisticated in masking their attacks.

High profile attacks in 2014 and 2015 all have seemed to contain one common element: some employee, either high-level, low-level, or one targeted specifically for his or her password and administrative privileges information, opened a malicious email which set off a catastrophic set of consequences for a company. Though there are many solutions that can be potentially employed to stop this pattern of doom and gloom, not one can be said to be entirely effective. Instead, the set of approaches described above, when used jointly, may help companies reduce the risk of potentially being spear phished “to death” by bad actors.

1. The existence of the first “snake-oil salesmen” date back at least to the time of the First Intercontinental Railroad in 1863.
recipients that their Automated Clearing House electronic-funds transfer was declined, and invites the recipient to click a link to “view the full details,” which leads to a Dropbox page that lists specific instructions, including the need to enable Microsoft Office macros).

10. See Verizon Report.

11. See, e.g. the comprehensive anti-phishing training services offered by www.phishme.com.


If you have questions concerning the contents of this issue, or would like more information about Weil’s Cybersecurity, Data Privacy & Information Management practice, please speak to your regular contact at Weil, or to the editors or authors listed below:

Editors:

Michael Epstein (NY)  Bio Page  michael.epstein@weil.com  +1 212 310 8432

Randi Singer (NY)  Bio Page  randi.singer@weil.com  +1 212 310 8152

Paul Ferrillo (NY)  Bio Page  paul.ferrillo@weil.com  +1 212 310 8372

Contributing Authors:

Paul Ferrillo (NY)  Bio Page  paul.ferrillo@weil.com  +1 212 310 8372

Randi Singer (NY)  Bio Page  randi.singer@weil.com  +1 212 310 8152

© 2015 Weil, Gotshal & Manges LLP. All rights reserved. Quotation with attribution is permitted. This publication provides general information and should not be used or taken as legal advice for specific situations that depend on the evaluation of precise factual circumstances. The views expressed in these articles reflect those of the authors and not necessarily the views of Weil, Gotshal & Manges LLP. If you would like to add a colleague to our mailing list, please click here. If you need to change or remove your name from our mailing list, send an email to weil.alerts@weil.com.