Combating Business Email Compromise

Sean Burns, MS
Retired FBI SSA

REGAL INVESTMENT ADVISORS™

Integrity • Innovation • Independence

Combating Business Email Compromise
Sean Burns, MS - Retired FBI SSA

Sean Burns retired from the FBI in January 2017 with over 25 years of investigative and supervisory experience. Mr. Burns started his career with the FBI in 1991 in Pittsburgh, PA, where he worked primarily narcotics and violent crime cases. He served as a team leader for the Pittsburgh Division's SWAT Team. In 2001, Mr. Burns was transferred to the Grand Rapids, MI, office where he primarily worked violent crime matters and was the Sniper Team Leader for the Detroit Division's SWAT Team. In 2012, Mr. Burns was promoted to Supervisory Special Agent, with territorial responsibilities that covered most of West and Northern Michigan. At the time of his retirement, Mr. Burns was a certified FBI instructor in the following disciplines: firearms, defensive tactics, tactical, tactical air officer, rappel master, and Crisis Management Coordinator. He has worked on numerous protection details for the FBI Director and U.S. Attorney General. As an FBI Special Agent, he was hand-selected twice for deployment to Afghanistan (2006, 2010) in support of the United States' global war on terrorism. Mr. Burns holds a Masters of Science degree from Grand Valley State University in Criminal Justice. He is a licensed professional investigator in the State of Michigan. Burns consults for Regal Investment Advisors and Regulus Advisors in a risk management capacity as a layer of security in compliance and recruiting onboarding.

In a previous article which discussed the FBI's Financial Fraud Kill Chain, I indicated my next essay would address ways that we can protect ourselves and our clients from the compromise of our email systems. With this article, I will attempt to fulfill that promise. In the pages that follow, I will address the issue of business email compromise (BEC) and how we can protect our clients, ourselves, and our company. But before we begin that discussion, we first need to define some terms.

Phishing, Spear-phishing, and Whaling Attacks

Phishing is a fraudulent process used by cyber-criminals to acquire sensitive information from users. This sensitive information can be usernames, passwords, and/or financial data, such as credit card details or bank account information. Recipients are often deceived by phishing attempts since messages appear to be sent by legitimate and trustworthy sources. Criminals attempt to make contact with victims via email, social media (e.g. Facebook), telephone calls (sometimes called "vishing" for voice-phishing), and text messaging (also referred to as "smishing" for SMS-phishing).[1] Cyber-criminals attempt to pose as a well-known organization or individual in order to obtain access to a target's account information. Once the criminal has the victim's passwords and account information, the attacker can use this information to access and clean out a victim's accounts. [2]

Spear-phishing is a specific type of phishing. It is a direct attempt to steal sensitive information from a specific target. That target can be an organization or an individual. When a spear-phishing attack is directed at executive management within a company or organization, it is also referred to as a "whaling" attack. These executives, or "whales," are chosen because of their outsized stature within their agency and because of their access to key accounts within the agency.[3]

This type of attack was utilized by members of the Russian Main Intelligence Directorate of the General Staff (GRU) during the US Presidential campaign in 2016 to hack into the computer of John Podesta. At the time of the attack, Podesta was the chairman of Hillary Clinton's Presidential Campaign. According to an indictment of 12 Russian military intelligence members filed by Special Counsel Robert Mueller on 13 July 2018, GRU officers sent Podesta a spear-phishing email that was crafted as a security notification from Google, the company that hosted the Democratic National Committee and the Democratic National Congressional Campaign email services. The spoof email provided a link for Podesta to change his password. Podesta's assistant, after consulting with a security technician, clicked on the link to change Mr. Podesta's password. Once that was done, Podesta's emails and the email servers of the DNC/DNCC were compromised. [4]

How an Attack Occurs

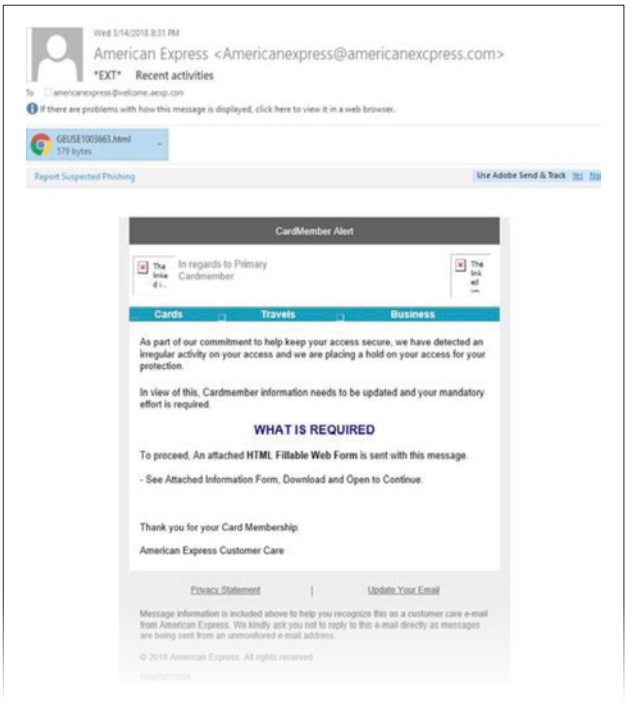
As noted above, spear-phishing and whaling attacks are targeted towards specific individuals because of their prominence within an organization. Phishing attacks are more diffuse. Phishing attacks are usually sent to large masses of people, generally at the same time. Attackers hope that someone will click on the link in the email, then provide their sensitive information to the link. In some attacks, rather than asking victims for their sensitive information, attackers will attach a link to malicious software ("malware"). The malware establishes itself on the victim's computer and provides the criminals with the victim's passwords and login data.

Although phishing attacks are more common, spear-phishing attacks are becoming more prevalent. Because spear-phishing attacks target specific individuals inside an organization, the emails have to contain more personal information concerning the target, in order for the target to believe the email is legitimate. Criminals will mine social media, both personal sites and agency sites, for information concerning their intended target. Spear-phishing attacks take more work for the criminals with regards to research, but the potential payoff is much greater. Because of the personal information contained in the emails, the spoofed email is harder to identify as fraudulent, and victims often provide the requested information.[5]

If you have not been the target of one of these attacks, you are in the minority. Chances are you have been targeted, but you did not realize it. The FBI's Internet Crime Complaint Center (IC3) has seen a 1300% increase in identified losses since January 2015, totaling over $3 billion.[6] Those are identified losses; they do not account for unknown losses or losses not reported to law enforcement.

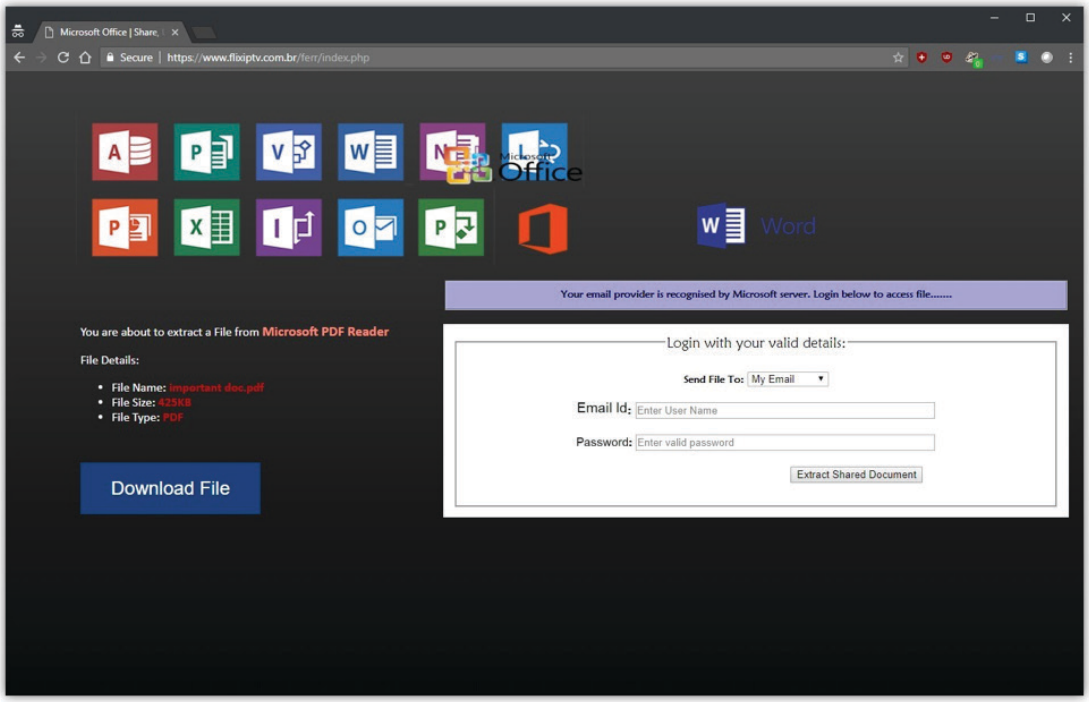
Our clients are also at risk, particularly clients who are seniors. Scammers frequently target senior citizens as they are not as "tech-savvy" as younger clients and seniors frequently have larger assets that thieves can target. Research has also shown that people become more vulnerable to fraud schemes as they age because their cognitive functions start to decline. [7]

The email to the right appeared a couple of weeks ago on one of my email accounts. I immediately was suspicious because I do not have an AMEX card. Some of the other indicators in the email are poor grammar and sentence structure in the body of the email; i.e. "we have detected an irregular activity on your access and are placing a hold on your access..." and "In view of this, Cardmember information need to be updated and your mandatory effort is required." Also, notice that the email address for American Express is changed slightly, by one letter: Americanexpress@americanexcpress.com contains a "c" between the "e" and "p" of "express". Victims will often miss this misspelling on first glance, especially if the email concerns an adverse outcome for the victim. Lastly, the email conveys an air of urgency, that it must be addressed quickly, or there will be a bad outcome for the person receiving the email.

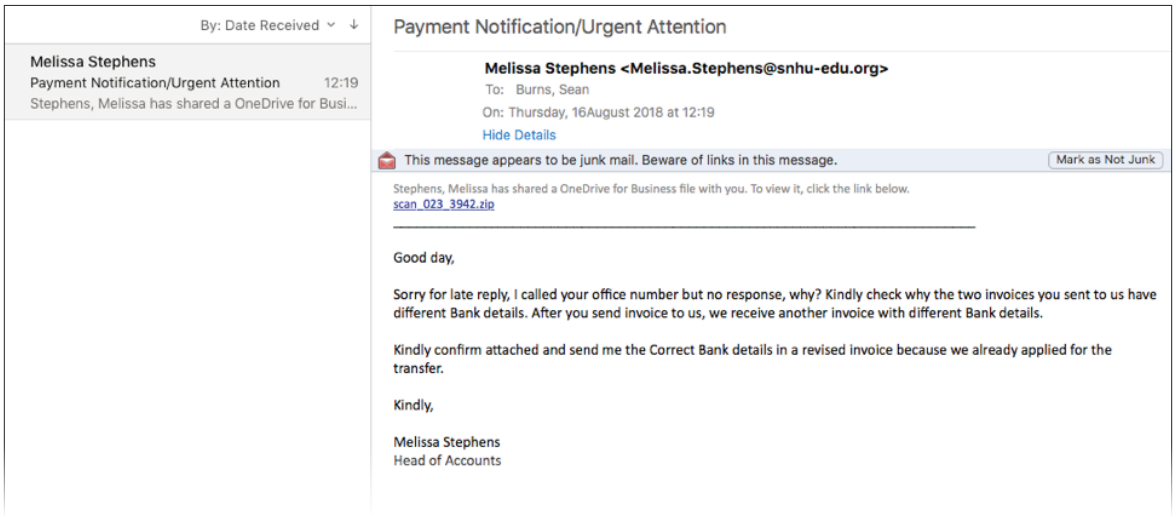


Oftentimes, clicking on links located in spoofed emails will redirect you to a website that is used to harvest your credentials. Below is an example that I recently came across.

Clicking on this link takes one to the following screen, which is set up to steal email information. By logging in with one's email ID and password, the victim has just given the cyber-thieves access to his/her account and access to the company's servers.



The next example is somewhat unique in that I received it while I was writing this article. In fact, it came to me on my Regal email account. Since I only use my Regal email account for communications within the Regal family, I immediately was suspicious. Also, the return email header/URL (snhu-edu.org, rather than snhu.edu), the lack of personal information in the email, and the fact that I had not done any business with Ms. Stephens also raised my suspicions and confirmed to me that this was a phishing attack. I notified our IT folks so they could alert others in the company. I later found out the message was part of a training session that the IT unit used to simulate an attack.



Defending Against Attacks

Below are proactive steps we all can take to further secure ourselves, our clients, and our company, online.[8]

- Place as little information on public social media sites as possible. For businesses, this includes company financial information and personnel information. For individuals (especially executives), this includes personal information such as travel schedules, friends, addresses, and family members. This information can be used by hackers for a whaling attack.
- Be suspicious of unsolicited phone calls, text messages, and emails asking about personal information or internal company information.
- Pay attention to the uniform resource locator (URL) of an email. This is the address from which the email was sent. Be wary of URLs that have a variation in spelling or a different domain (e.g. .con vs .com).
- Establish two-factor authentication for transfers of money. Confirm wire transfers with telephone calls to known numbers for voice verification of the transfer or confirm the transfer face-to-face. I had a case when I was an Agent in which a Chief Financial Officer approved a significant fraudulent wire transfer because he had received what he believed was a legitimate email from the CEO authorizing the transfer. The attackers had done their homework on social media — they knew the CEO was on vacation in the Bahamas. The CFO approved the transfer without checking with the CEO. Fortunately, an employee noticed the URL on the CEO's authorization email was slightly different than the company's address (.orq instead of .org) and the transfer was not sent.
- Mark emails coming in from external servers. Many phishing attacks are engineered to look like they came from someone within the company. Flag emails from outside the company with a banner marking the email as coming from an external source. Emails from outside the company can also be color-coded so they are a different color than internal emails.

These are small, but significant steps, that we all can take to ensure that our clients, ourselves, and the people we work with, do not become the victims of email phishing scams.

Citations

[1] Giandomenico, 2018.

[2] Avoiding social engineering and phishing attacks, 2017.

[3] Giandomenico, 2017.

[4] Nakashima & Harris, 2018.

[5] Federal Bureau of Investigation, 2017; Giandomenico, 2018.

[6] FBI, 2017

[7] How to help clients avoid fraud. 2018

[8] Avoiding social engineering and phishing attacks, 2017; FBI, 2017; Giandomenico, 2017; Giandomenico, 2018.

References

How to help clients avoid fraud. (2018). Retrieved from https://www.wealthmanagement.com/white-papers/how-help-clients-avoid-fraud

Avoiding social engineering and phishing attacks [Press release]. (2017, January 24). Retrieved from https://www.us-cert.gov/ncas/tips/ST04-014

Federal Bureau of Investigation. (2017, February 27). *Business e-mail compromise: Cyber-enabled financial fraud on rise globally* [Press release]. Retrieved from https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise

Giandomenico, N. (2017). What is a whaling attack? Defining and identifying whaling attacks. Retrieved from https://digitalguardian.com/blog/what-whaling-attack-defining-and-identifying-whaling-attacks

Giandomenico, N. (2018). What is spear-phishing? Defining and differentiating spear-phishing from phishing. Retrieved from https://digitalguardian.com/blog/what-is-spear-phishing-defining-and-differentiating-spear-phishing-and-phishing

Nakashima, E., & Harris, S. (2018). How the Russians hacked the DNC and passed its emails to WikiLeaks. Retrieved from https://www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html?utm_term=.349920fbc717

Satter, R. (2017). Inside story: How Russians hacked the Democrats' emails. Retrieved from https://www.apnews.com/dea73efc01594839957c3c9a6c962b8a

2687 44th Street SE | Kentwood, MI 49512 | 800.357.4757 | **regalfin.com**