Robinhood Breach Underscores the Dangers of Social Engineering

By Sharon D. Nelson, Esq., John W. Simek and Michael C. Maschke

From Robin Hood to Robinhood

We all remember the legendary heroic outlaw Robin Hood who made it his mission to rob the rich and give to the poor. Robinhood, a financial services company which seemed to take a page from Robin Hood, declared its mission "to provide everyone with access to financial markets, not just the wealthy" with a no-fee trading application. In early November 2021, it experienced a data breach. Roughly seven million accounts were compromised. Mostly email addresses were leaked and more serious data for about 300 clients.

Lessons in Social Engineering from the Robinhood Breach

Apparently, the cybercriminal who attacked Robinhood contacted a Robinhood customer support worker, convinced that worker to divulge information and/or take actions which allowed the attacker to gain access to some support systems. Though it appears that mostly email addresses were compromised (though some more significant data for a small number of clients), this is not precisely a "ho-hum, that wasn't so bad" sort of result. Mind you, it could have been much, much worse.

It should be noted that, at a minimum, it is likely that those compromised email addresses will be used for targeting phishing attacks. We don't know whether Robinhood gave this specific advice to those compromised, but Robinhood users should immediately change their passwords, enable two-factor authentication and be on the lookout for suspicious emails.

Law firms should heed well the fact that that social engineering (via a fallible human being) resulted in the breach.

Why Do Law Firms Pay Relatively Short Shrift to Social Engineering Attacks?

Frankly, we've never been able to figure this out. Law firms will invest a ton of money in security technology and give relatively short shrift to training their employees about cybersecurity, including social engineering attacks.

The omission to train in-depth and often is glaring, especially when a 2020 joint study by Stanford University and security firm Tessian demonstrated that 88% of data breach incidents involve human error. The lowest figure we've ever seen in any study is 82%. Certainly, those numbers should command the attention of law firm management.

Real—life Examples of Law Firm Social Engineering

There's an endless list but let's start with a few:

1. Attacker calls someone at the law firm, perhaps talking to the receptionist. They ask for the name of the Chief Financial Officer or simply the person who pays the law firm's bills – maybe they suggest they have a billing question or a complaint. Most of the time, the receptionist will identify those people to the caller and now they have the names of people they could target as

part of a wire fraud scheme.

2. Perhaps the attacker calls and exclaims “I’ve heard that you have a great IT support company. Who do you use? I want to give them a call.” The person answering the phone innocently gives out that information. Bad guys look up the company, perhaps select a name or two from the website and pretends to be from your IT company, with an urgent request from the managing partner (we make it easy to find those names). The attacker presents a hapless employee with a system change that needs to be made by close of business (and of course that’s when they call) and needs the employee’s password and ID. Employee, believing it is their IT company, complies. If this column had sound effects, you would hear the sound of a planet imploding.

3. Over the weekend, when attorneys are not likely to be in the office, an attorney gets a call from Microsoft (not) or Apple (not) at home or on their cell phone saying that they have identified a threat actor (or something else that sounds dangerous) in their laptop. They direct the attorney to go someplace in the laptop which may show something that looks like a bona fide problem. (Typically, innocuous warnings/errors appear in a log file.) While they are in the process of “fixing the problem,” they are actually owning the machine and installing malware. When that laptop joins to the network, “KABOOM.”

4. The most notorious kind of social engineering is phishing emails (and increasingly, phishing texts). While there are a lot of amateurish phishing emails, replete with spelling errors and atrocious grammar, cybercriminal gangs are getting smarter, hiring people who natively speak American English, British English, Canadian English, Australian English, etc. Targeting law firms, which are rich in the data of many people and businesses, has been a tried-and-true attack vector for cybercriminals.

   Successful phishing subject lines included these in the top 10 for 2021:

   a. Password Check Required Immediately
   b. Vacation Policy Update
   c. Important: Dress Code Changes
   d. ACH Payment Receipt
   e. Test of the (insert law firm name) Emergency Notification System
   f. Scheduled Server Maintenance – No Internet Access
   g. COVID-10 Remote Work Policy Update
   h. Scanned Image from (insert domain name)
   i. Security Alert
   j. Failed Delivery

5. Phishing emails have “grown up” and changed form often delivered as a text message to your smartphone. This is known as a Smishing (phishing via SMS text message) attack. Perhaps you received a text message purportedly from AT&T thanking you for your recent payment with a link to retrieve “your thank you gift.” Click the link and you’ll receive the “gift” of malware. Or you get a text message appearing to come from your credit card company warning of a potential

fraudulent charge. They very conveniently provide a link sending you to a website where you can report the fraud and confirm your account information, which will allow for a boatload of real fraudulent charges.

Last words

In Proofpoint's State of the Phish 2021 report, 57% of all respondents experienced a successful phishing attack. That's a high number – and certainly justifies a continuing emphasis on cybersecurity awareness training for employees.

Periodic reminders to law firm employees supplement the training as do regular phishing simulations, which very inexpensively demonstrate which law firm employees are most dangerous to the firm and require remedial education.

To quote Sun Tzu, "The opportunity of defeating the enemy is provided by the enemy himself." Use what your enemy gives you!

Sharon D. Nelson *is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA.* *snelson@senseient.com*

John W. Simek *is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH) and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm.* *jsimek@senseient.com*.

Michael C. Maschke *is the CEO/Director of Cybersecurity and Digital Forensics of Sensei Enterprises, Inc. He is an EnCase Certified Examiner, a Certified Computer Examiner (CCE #744) a Certified Ethical Hacker and an AccessData Certified Examiner. He is also a Certified Information Systems Security Professional.* *mmaschke@senseient.com*.