Mind Games Cybercriminals Play with Law Firm Employees

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

"Hackers Don't Break In, They Log In"

We love that quote from Corey Nachreiner, the CSO of cybersecurity firm WatchGuard. We do of course make logging in all too easy. Many law firms do not have an out-processing checklist for those who leave their employment, so we make it simple to discover Ids and passwords that are "hanging around."

If they reused their passwords, they make it even easier for the attackers. But a current ploy is simply to pretend that they are someone else (usually another law firm employee) and indicate the need for the ID/password for any number of reasons — a network threat they are working on or involvement in a compilation of Ids/passwords to be stored securely in the cloud to enhance (they say) security.

They may even pretend to be your IT provider and they need your credentials to counter an imminent threat that has just been discovered. A remarkable number of law firm employees will give up their credentials in their desire to be helpful to someone they presume to be legitimate.

Are we saps? Pretty much, based on the evidence.

But We're Using 2FA, So We're OK, Right?

Wrong. Take a recent case from the headlines, the Uber breach. First, the hacker pretended to be a fellow employee and got credentials which permitted access to the network — but 2FA was enabled. Then the hacker bombarded the hapless employee with push notifications asking that they confirm a remote log-in to their account.

When the employee did not respond, the hacker reached out via WhatsApp posing as a fellow worker from the IT department and expressing urgency. Ultimately, the employee gave in and confirmed with a mouse click. D'oh.

Imagine a similar attack in a law firm with 2FA enabled. How many times will the employee reject a string of "confirm" requests before they get sick of clicking dismiss and give in to clicking 'Accept'?

Wearing someone down isn't a sophisticated tactic, but here and elsewhere, we've seen it work. Just keep hammering them until they succumb to push fatigue.

Furthermore, "Attackers are getting better at by-passing or hi-jacking MFA (multi-factor authentication)," said Ryan Sherstobitof, a senior threat analyst at SecurityScorecard.

That's why many security professionals suggest the use of so-called FIDO (Fast Identity Online) physical security keys for user authentication. The YubiKey is one example of these physical security tokens. Google employees utilize a Titan Key and claim they've never had their accounts hacked since 2017. Adoption of such hardware has been all but non-existent in law firms.

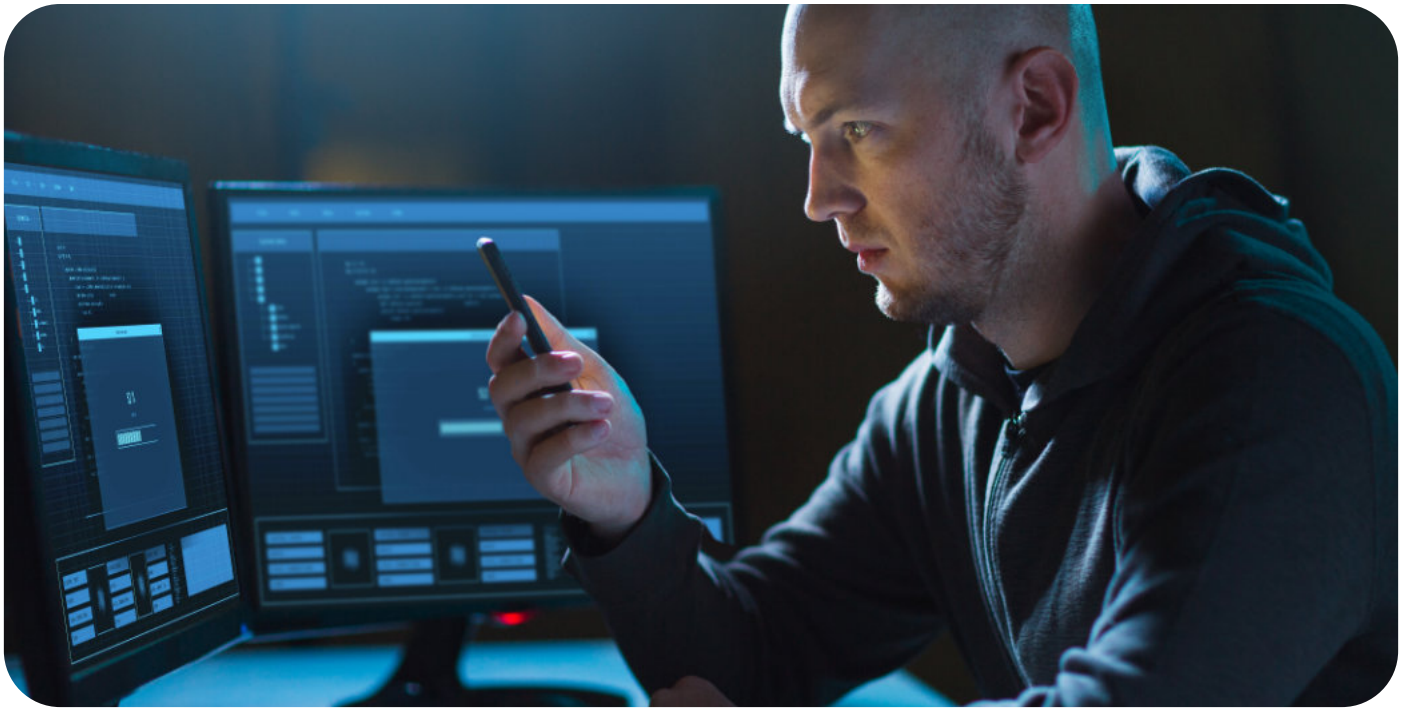
Chalk up a victory for the bad guys.

Hackers Using Fake Jobs in Phishing Attacks

LinkedIn is now awash in phony accounts, many of them created in the last several months as a new scam emerges. Some of the accounts are run by people who make bogus job offers, persuading job applicants (who may be currently working for you) to install WhatsApp where they then share a Trojan. A highly targeted group is IT employees. That should be a serious "uh-oh" for law firms.

Microsoft-owned LinkedIn is trying hard to get a handle on these bogus accounts but it's a game of Whac-a-mole.

In 2021, U.S. authorities warned U.S. firms to be wary of IT contractors applying for support and developer roles — noting that they may use faked social media accounts as validation of who they are.



Cybercriminals Will Pay Your Employees for Data — Will They Say No?

That's an excellent question. We have already seen 18% of hospital workers acknowledge in a survey that they would sell confidential data for $500 - $1000. 21% of those in 'provider' organizations indicated that they would sell login credentials, install tracking software or download data into a portable drive and send it off to the buyter. So much for integrity.

Scary? Yes indeed. And do you really think that all law firm employees would be impervious to being offered money for data? We hope not. Needless to say (but we will), the cybercriminals do not tell employees how they will use the data, often pretending a relatively innocent reason for paying for the data (for instance, using it for marketing purposes).

How many times have law firms reported that departing attorneys took firm data to their new employers? That is regularly a story in the news. They may not be "selling" it per se but having it may be alluring to the new law firm which hired them. What precautions, if any, has your law firm taken against such actions?

Using Deepfakes to Access Your Network (or Get You to Wire Funds)

For a long time, we have seen Business Email Compromise (BEC) attacks, where cybercriminals hack into accounts belonging to managing partners — or spoof their email accounts and ask an authorized employee to wire large sums of money to a bank.

The emails are always urgent — which should be a red flag, but that flag is clearly invisible to many people authorized to wire funds. Of course, such requests should always be regarded with suspicion and independent confirmation should be made by walking down the hall or calling the partner authorizing the wiring of funds at a known good number. But that's not what many law firms do.

Sadly, by the time folks become suspicious, the cybercriminals have the money in hand, probably closed the bank account they used — and evaporated into thin air.

Now, as BEC becomes aknown threat to law firms, they are getting smarter — but the cybercriminals are upping their game. What if the criminals use a deepfake of a managing partner to make the wiring request via a video conference?

Our friend, Oklahoma practice manager advisor Jim Calloway, had the same thought in September 2022 when he wrote a column called "The Next Big Security Threat is Surprising and Scary." It's not just law firm higher ups who might make this kind of request. Frequently, a client will authorize the wiring of monies — what if the deepfake is a client on a Zoom call?

Cybersecurity Awareness Training for Employees: Do it Well and Often

As you might imagine, we could go on and on with scary stories, which is perhaps appropriate given that Halloween is coming up. So how do you combat the scary stuff?

Policies about what you should do in given circumstances are great — and by all means develop them. But they are not top of mind for most employees.

Because the threats and the defenses against them change so rapidly, we urge law firms to do mandatory cybersecurity awareness training regularly, specifically so you can educate employees on the new threats and sensitize them to the tactics of cybercriminals, especially on some of the social engineering tactics cited above. Bonus news — your cyber insurance carrier may require annual or semi-annual security awareness training to obtain cybersecurity coverage.

We have been lecturing for several years on BEC and wire fraud. But these new tactics of using deepfakes — and fake social media accounts — have only been in the news quite recently. The takeaway for us is that we need, yet again, to update our PowerPoint. But the lesson for law firms is that defending your firm data depends on monitoring all the new ploys, including the mind games, that cybercriminals are employing to get your data — and the monies you hold in trust.

The Last Words Go to Albert Einstein

"Only two things are infinite, the universe and human stupidity, and I'm not sure about the former."

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, Certified Ethical Hacker, and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity, and digital forensic services from their Fairfax, Virginia firm.* jsimek@senseient.com

Michael C. Maschke *is the CEO/Director of Cybersecurity 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