Feature

Gone Phishing: How Law Firms Can Thwart Cyber Hustlers

*By **Aebra Coe***

Law360 (February 15, 2019, 5:20 PM EST) -- While cyberattacks may come via email or social media, the underlying crime is one of human deception that could have occurred in the past by phone or in person. Yet the high-tech nature of such scams may make them harder to sniff out, with a recent case of a Dentons attorney being a cautionary tale.

The fraud targeting the global firm was spelled out in a December decision by an Ontario, Canada, court, which was weighing an insurance claim the firm made to recover stolen funds.

An associate at Dentons' Canadian arm had wired $2.5 million of a client's money to a Hong Kong bank account — set up by cybercriminals — during the course of a real estate transaction, after receiving emails from fraudsters pretending to be legitimate employees of a mortgage company, according to the decision.

A number of law firms in recent years have been hit with such attacks, in which a criminal poses as someone the victim would normally trust and share information with. Attorneys must have safeguards in place and know how to spot red flags in order to avoid "blindly transferring large sums of cash to criminals," according to Eyal Benishti, founder and CEO of security technology company IronScales.

"Business email compromise attacks are proving lucrative and increasingly successful," he said. "It's pure social engineering via email trying to redirect large sums of money."

Useful Tools & Links

Add to Briefcase
Save to PDF & Print
Rights/Reprints
Editorial Contacts

Related Sections

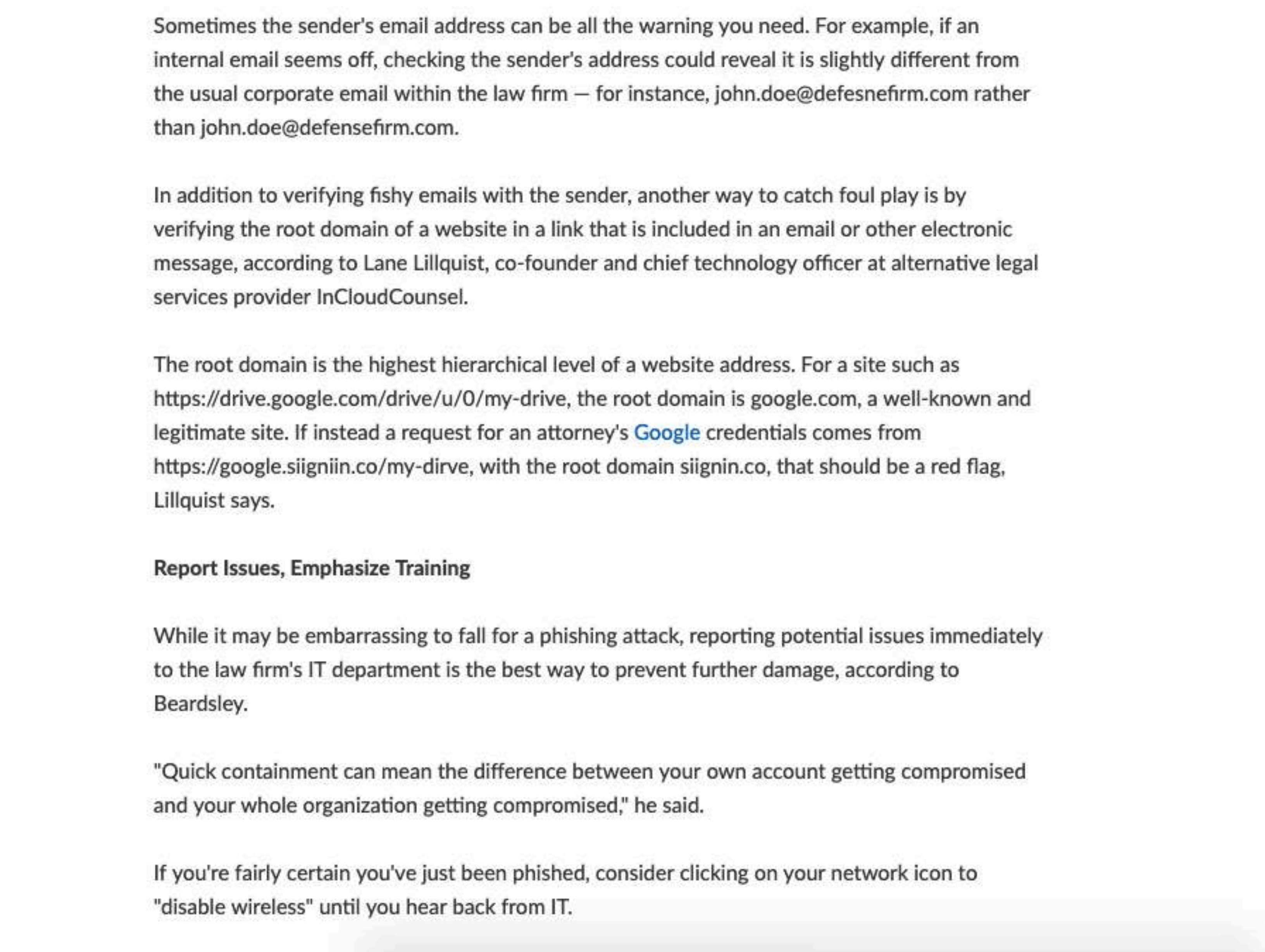
Legal Industry

Law Firms

Dentons

Companies

Amazon.com Inc.
Google Inc.
Mimecast Ltd.
Rapid7 Inc.



Sometimes the sender's email address can be all the warning you need. For example, if an internal email seems off, checking the sender's address could reveal it is slightly different from the usual corporate email within the law firm — for instance, john.doe@defesnefirm.com rather than john.doe@defensefirm.com.

In addition to verifying fishy emails with the sender, another way to catch foul play is by verifying the root domain of a website in a link that is included in an email or other electronic message, according to Lane Lillquist, co-founder and chief technology officer at alternative legal services provider InCloudCounsel.

The root domain is the highest hierarchical level of a website address. For a site such as https://drive.google.com/drive/u/0/my-drive, the root domain is google.com, a well-known and legitimate site. If instead a request for an attorney's Google credentials comes from https://google.siigniin.co/my-dirve, with the root domain siignin.co, that should be a red flag, Lillquist says.

Report Issues, Emphasize Training

While it may be embarrassing to fall for a phishing attack, reporting potential issues immediately to the law firm's IT department is the best way to prevent further damage, according to Beardsley.

"Quick containment can mean the difference between your own account getting compromised and your whole organization getting compromised," he said.

If you're fairly certain you've just been phished, consider clicking on your network icon to "disable wireless" until you hear back from IT.

"But don't beat yourself up over it. Phishing happens; it's effective, and part of its effectiveness is due to people not self-reporting when they fall for it," he added.

As organizations, law firms can focus on education as one important way to prevent cyberattacks and make sure employees understand how to respond if they are tricked. A number of outside companies provide training for organizations in cyberattack prevention.

Firms should provide cybersecurity training to all staff and attorneys when they are hired and at least once a year after that, Lillquist suggests.

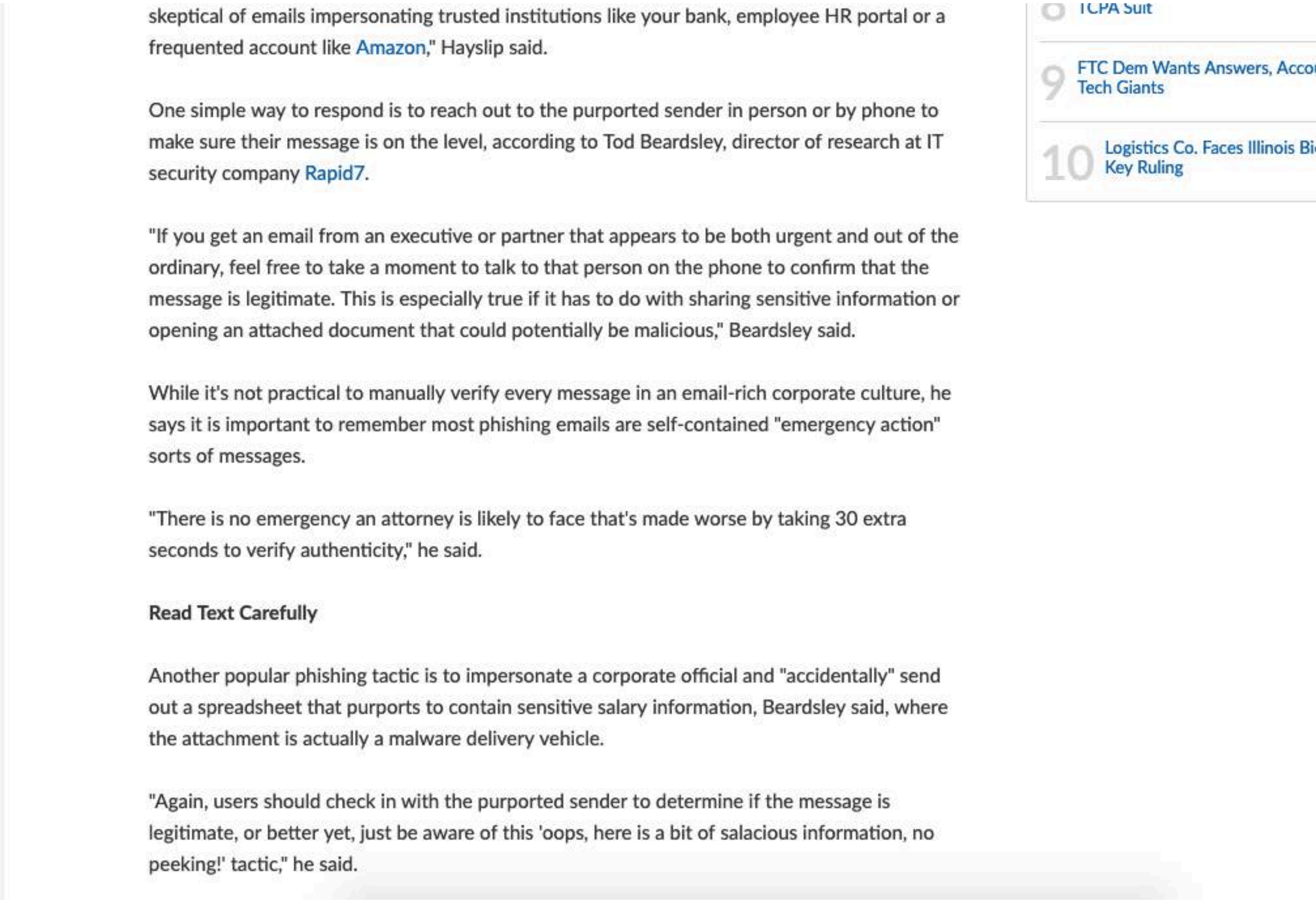
Use Safeguards

Raising employee awareness to phishing indicators so that fewer are duped into falling for scams in the first place is a solid foundation, but that alone is not enough, according to IronScales' Benishti.

Anti-impersonation technology and sender reputation scoring can monitor communication habits, at the inbox level, to build a picture of what normal communications look like, Benishti explained. Then, anything that stands out as different can be identified and visually flagged as a potential malicious impersonation attempt.

"This sounds a warning bell to the user which might make the difference between them questioning the message's intention or blindly transferring large sums of cash to criminals," he said.

Other technological safeguards law firms can turn to, according to Sloshberg, include technical anti-phishing defenses, secure messaging and core security controls such as multifactor authentication and endpoint security systems.



skeptical of emails impersonating trusted institutions like your bank, employee HR portal or a frequented account like Amazon," Hayslip said.

One simple way to respond is to reach out to the purported sender in person or by phone to make sure their message is on the level, according to Tod Beardsley, director of research at IT security company Rapid7.

"If you get an email from an executive or partner that appears to be both urgent and out of the ordinary, feel free to take a moment to talk to that person on the phone to confirm that the message is legitimate. This is especially true if it has to do with sharing sensitive information or opening an attached document that could potentially be malicious," Beardsley said.

While it's not practical to manually verify every message in an email-rich corporate culture, he says it is important to remember most phishing emails are self-contained "emergency action" sorts of messages.

"There is no emergency an attorney is likely to face that's made worse by taking 30 extra seconds to verify authenticity," he said.

Read Text Carefully

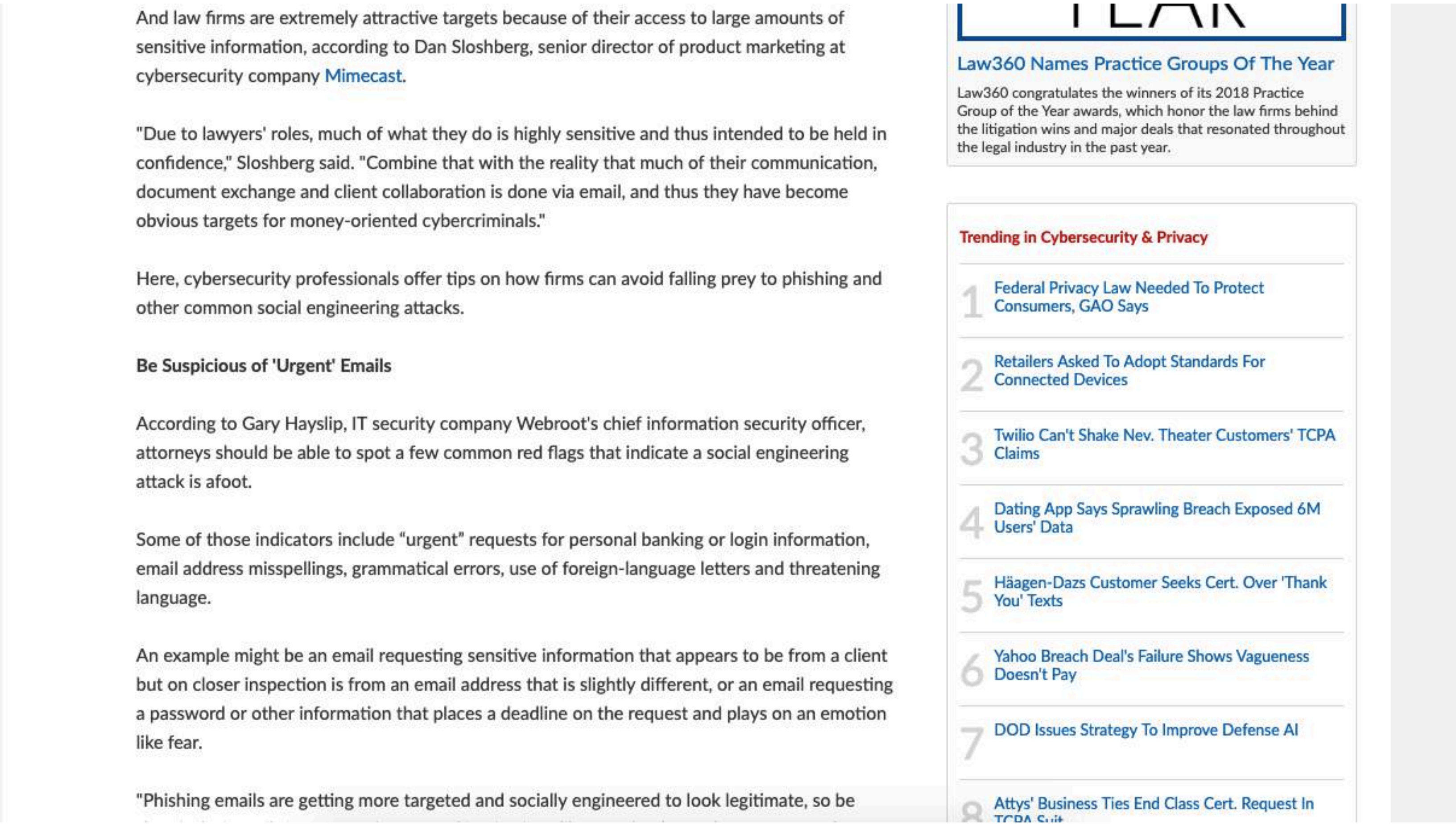
Another popular phishing tactic is to impersonate a corporate official and "accidentally" send out a spreadsheet that purports to contain sensitive salary information, Beardsley said, where the attachment is actually a malware delivery vehicle.

"Again, users should check in with the purported sender to determine if the message is legitimate, or better yet, just be aware of this 'oops, here is a bit of salacious information, no peeking!' tactic," he said.

8 TCPA Suit

9 FTC Dem Wants Answers, Acco
Tech Giants

10 Logistics Co. Faces Illinois Bi
Key Ruling



And law firms are extremely attractive targets because of their access to large amounts of sensitive information, according to Dan Sloshberg, senior director of product marketing at cybersecurity company Mimecast.

"Due to lawyers' roles, much of what they do is highly sensitive and thus intended to be held in confidence," Sloshberg said. "Combine that with the reality that much of their communication, document exchange and client collaboration is done via email, and thus they have become obvious targets for money-oriented cybercriminals."

Here, cybersecurity professionals offer tips on how firms can avoid falling prey to phishing and other common social engineering attacks.

Be Suspicious of 'Urgent' Emails

According to Gary Hayslip, IT security company Webroot's chief information security officer, attorneys should be able to spot a few common red flags that indicate a social engineering attack is afoot.

Some of those indicators include "urgent" requests for personal banking or login information, email address misspellings, grammatical errors, use of foreign-language letters and threatening language.

An example might be an email requesting sensitive information that appears to be from a client but on closer inspection is from an email address that is slightly different, or an email requesting a password or other information that places a deadline on the request and plays on an emotion like fear.

"Phishing emails are getting more targeted and socially engineered to look legitimate, so be

Trending in Cybersecurity & Privacy

1 Federal Privacy Law Needed To Protect Consumers, GAO Says

2 Retailers Asked To Adopt Standards For Connected Devices

3 Twilio Can't Shake Nev. Theater Customers' TCPA Claims

4 Dating App Says Sprawling Breach Exposed 6M Users' Data

5 Häagen-Dazs Customer Seeks Cert. Over 'Thank You' Texts

6 Yahoo Breach Deal's Failure Shows Vagueness Doesn't Pay

7 DOD Issues Strategy To Improve Defense AI

8 Attys' Business Ties End Class Cert. Request In TCPA Suit

"Even using a password manager is a good practice, as it will help ensure the same passwords are not used for multiple systems and are also not auto-filling on a phishing site that looks like the real one, for example," he said.

--Editing by Breda Lund and Philip Shea.

0 Comments

Commenting enabled only for paid accounts