Hooked by Spear Phishing Bait: An Easy Catch

Anatomy of a Spear Phishing Attack

XO Legal, a small legal firm with an entirely distributed team, was lured into a spear phisher's snare. The insidious phishing attack targeted the firm with carefully crafted emails that appeared to come from legitimate and trusted internal sources. This sleight of email was virtually undetectable. *XO Legal had no idea how to pick up the pieces because they didn't know what the pieces were.*

Spear Phishing Prey

Once the phisher had decided on a law firm target, XO Legal, they did what any highly skilled phisher would do: They patiently researched the firm, its employees, clients, and ongoing cases to gather information that would make their phishing email(s) appear authentic and relevant.

Excellent dossiers were created on all the firm’s employees. From the information acquired, partners Xavier Otero and Rogelio Tejada seemed to be the most potentially profitable targets. The phisher decided to reference a high-profile client as part of the deception. They had learned that there was a hearing the following week, which provided the opportunity to introduce urgency and authenticity into an email.

The spear phisher registered two email addresses using a free email service, carefully selecting usernames that incorporated the names of the attorneys and the firm's domain name. They had managed to find out the name of the cloud storage company. The rest was frighteningly simple.

It was this meticulous preparation that enabled the phisher to craft the personalized emails that would become the bait and make this plot so successful. Their chances of success were greatly improved because the plot was entirely specific to the XO Legal firm.

The Attack

> We thought our client information was secure--until it wasn't...
>
> **Xavier Otero, Partner, XO Legal**

An email was sent to one of the paralegals, Ana Mathieson, from Xavier Otero. The email referred to an upcoming hearing the next day, for which Xavier Otero was the lead attorney. It requested that she look for a file in the client's folder. If it was there, he needed the link to it right away. He was on his smartphone right now and had no way to access the file. The email contained details about the hearing that she knew to be true. She hesitated but the first one was followed by two other emails, each more frantic than the last. Ana found the file and sent the link to the folder.

With this information alone, the spear phisher was able to access the client's information.

How did the spear phisher gain access to the file via shared link? Here is what the access protocols did not require for a link to a shared file:

- A password to access the file
- Authentication with the cloud service using account credentials
- Accept certain access permissions like view-only or edit permissions
- Multifactor authentication

The spear phisher was content with access to this one client's information. What they wanted was enough information to enable identity theft. There was plenty of information in the file to allow them to do that.

The Aftermath

XO Legal was forced to pay for all of the client's identity theft remediation, lost the client (which was a substantial part of their revenue). And in the end, they still did not know if any other client information had been breached. But it could have been far worse and far more costly.

A Zero Trust Mindset

The Zero Trust mindset is a new one for this firm because it is so small, and the staff knows

one another so well. But now they know that zero trust is critical if they are going to protect themselves and their clients. Now the company mantra is: *Never trust, always verify*.

Protecting client data--whether dictated by law or not--was of paramount concern at XO Legal. But, as with many firms, the *intention* of the staff to guard the sanctity of client data was not enough. Transformation into a team with a zero-trust mindset was essential. So, XO Legal closed the gaping voids in their security protocols with the following actions (non-inclusive):

Written Information Security Plan (WISP) to define what the firm's information assets are and how they will be protected--including the policies and procedures that will be used.

Incident Response Plan based on ABA Formal Opinion No. 483, which defines the lawyer's ethical and legal obligations to be prepared to protect against and respond to a cyber security incident.

Standard Operating Procedures were created for the Incident Response Plan and Written Information Security Plan, as required. One of the first ones written is how internal communications were treated,

User and Device Security is enforced by ensuring that all users and devices (including mobile devices) have the same level of protection as they access resources, regardless of location.

DMARC (Domain-based Message Authentication, Reporting, and Conformance) email authentication protocol is used to protect against email phishing.

Multifactor Authentication is mandatory for all staff who access files. In this case, fingerprint identification is used. **Application and Data Security** is used to prevent unauthorized access within app environments.

Ongoing Evaluation of Access and Authentication Protocols to ensure that permissions are appropriate and are updated, as necessary. It only one malicious link or attachment.

No law firm, regardless of its size, can afford to overlook the importance of cybersecurity. The increasing frequency of cyber-attacks targeting the legal sector is alarming, especially given the vast amounts of money, information, and client data law firms retain. Despite the growing awareness of cyber threats, many firms still lack a comprehensive understanding of the necessary precautionary measures to mitigate risks. This underscores the critical need for law firms to invest in cybersecurity and educate their employees on the best practices to protect sensitive information.

Contact Us: swbsconsultants@gmail.com