Don't Take the Bait! "Spear Phishing" and "Whaling" Take Scams to the Next Level

Insights
1.28.19

For several years now, we've been alerting employers about the dangers of phishing scams that attempt to obtain private and personal information from employers. See some of our previous posts here, here here, and here. Many of these scams rear their ugly head around tax season, with attacks targeting human resources staff and payroll personnel in particular.

However, hackers and scammers have taken their game to the next level. The degree of sophistication and targeting of these scams has risen to unprecedented levels of late. In fact, the progression of these attacks has even coined new terms to refer to them – "spear phishing" and "whaling."

So What Are "Spear Fishing" and "Whaling?"
We've probably all received general "phishing" emails in our professional and personal lives. These are generic emails sent out, purporting to come from retailers, health care providers, banks, and other businesses that try to trick you into providing personal information. Such emails are so ubiquitous that most of us can easily avoid and disregard them, even without a specific warning from the business to be on the lookout for a particular threat.

However, as highlighted in a recent great article in *CSO Online*, "spear phishing" and "whaling" are much more sophisticated and targeted attacks that are designed to provide much "greater" results for the scammers.

"Spear phishing" refers to schemes where the scammers engage in significant research to target individuals specifically through emails that purport to be sent by a trusted contact or colleague. In the past, such scams either tried to pass along malware through infected documents and attachments or attempted to obtain private and confidential information by tricking the recipient into believing they were legitimate requests for information.

But these schemes have become ever more sophisticated of late, sometimes using legitimate sites like Dropbox or Google Drive to house documents infected with malware.

"Whaling" refers to phishing schemes that go after high-level executives or officials. For example, a hacker may try to impersonate a company president, CEO, financial officer, HR officer, or similarly "important" person to try to convince a lower-level victim within the company to respond. This type

of attack takes a significant amount of research and planning. However, for many companies, information about corporate leadership is easily available on company websites, making it easier for attackers to select and target their victims.

Even law firms have fallen victim to such attempted "spear phishing" and "whaling" attacks. A common scam will involve someone impersonating a senior partner in a law firm with a "panicked" email to an associate claiming the partner is in a deposition or with a client, and needs the associate to rush out and purchase gift cards (and text pictures of the card numbers) because they need them as soon as possible to close a deal or settle a case.

Other schemes have targeted churches or houses of worship. Targeted emails purportedly coming from the local priest, rabbi, pastor or other church leader are sent to parishioners asking for money or gift cards for church repairs, missionary or charitable activities, or personal emergencies. Many churches have online parishioner directories, making their members ripe for the picking for such scams.

Don't Be Caught Hook, Line and Sinker!
So what's an employer to do in light of the increasing sophistication of such threats?

First, employers (and their employees) should be on the lookout for some common clues to spot "spear phishing" or "whaling" emails. These include:

- Poor spelling and grammar.
- Use of terms that are not normally used in your industry or don't fit your corporate culture.
- Unexpected or out of place messages. Beware of "urgent" or "emergency" messages asking recipients to perform some type of unusual or unprecedented task.
- Attempting to elicit some sort of emotion (such as sympathy or fear).
- Unfamiliar sender.
- Unfamiliar URL.
- A statement from the purported sender that he/she is unavailable to talk.

Beyond looking out for common clues, there are some general policies and practices employers should implement to minimize the degree of risk from such attacks. These include:

- Employers should immediately warn employees about the risks associated with these scams. The notice and appropriate training should be given to payroll, human resources, and any other group of employees with access to personally identifiable information to be on the lookout for these phishing attempts or other red flags, such as requests for information not typically requested, or requests from individuals with whom the employees do not typically directly communicate.

- Employers should remind employees not to open emails that come from a sender they do not know, are unsolicited, ask for their login credentials, include imbedded downloads or simply look suspicious.
- Employers should discourage use of company email accounts for personal use, such as online banking, credit cards and tax preparation services.
- Employers should change password access at least every few months and at unpredictable times.
- Employers should notify employees to be on the lookout for emails requesting personal and/or financial information for the company or a group of employees that appear to come from a supervisor. Employees should be directed to verbally follow up on such requests with the supervisor, and any phishing emails should be reported to the IT department.
- This also applies to employees who deal with clients, contractors or vendors. Employees should confirm any requests for sensitive information or payment with the client or other third parties directly before simply responding to an email.
- Employers should notify employees that requests from government agencies for personal and/or financial information for company employees or clients must go through a designated department or member of management.
- Employers should also take steps to limit the number of employees who have authority to access and disclose such information, and to implement procedures requiring validation of any request for sensitive personal data, such as Form W-2s, as well as any requests for wire transfers.

Finally, employers should invest in the installation of sophisticated technological barriers against unauthorized users gaining access to their data. Some providers now perform phishing simulation tests to evaluate your current system. But employers should never overlook the human risk factor. Following the tips above should help employers develop a "human firewall" that may ultimately be more important in the long term than any software or system you can purchase.

Oops! What Now?

Obviously, an employer's primary focus should be to avoid such "spear phishing" and "whaling" schemes and prevent a data breach from occurring in the first place.

But what if the worst case scenario happens and your company falls victim to such an attack? Employers who have fallen for these scams may be subject to data breach notification requirements. These obligations can vary from state to state, and employers should consult their counsel to identify applicable notification requirements.

Employers should also report any data breach to local law enforcement, as well as the FBI. In fact, many insurance companies may require this to occur anyway. Additionally, employers who may have fallen victim to these scams (particularly involving payroll or tax information) should consider notifying the IRS. The IRS has established a special email notification address specifically for

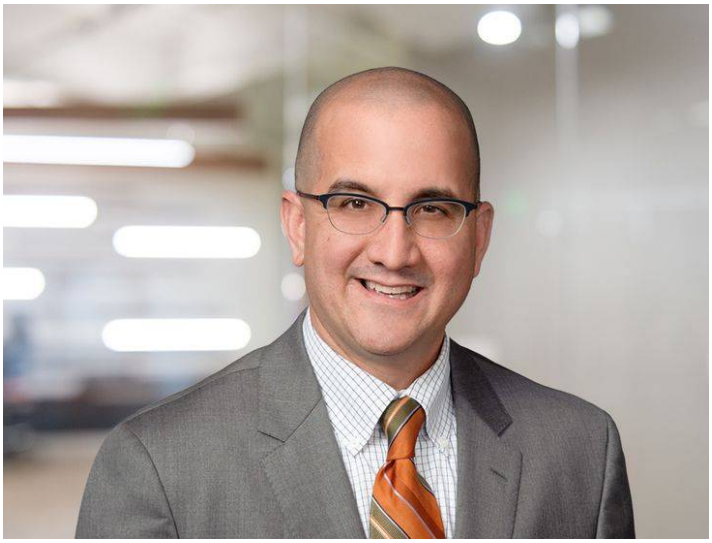
employers to report Form W-2 data thefts. Information about the procedure for submitting such reports, as well as the full text of the latest IRS notice to employers regarding this scam, is available here.

Employers should also consider arranging for an independent security audit following any breach. This involves hiring an outside consultant to analyze the company's internal systems and protocols, identify gaps, and recommend additional security measures. From a legal perspective, these steps can help to demonstrate that the employer is doing everything possible to mitigate damage and prevent future similar incidents.

Employers should consider (and some state laws may actually require) providing credit monitoring or other services to employees whose data may have been compromised in such an event.

For more information about how to protect yourself from such attacks, or what to do when an unfortunate breach occurs, contact any Fisher Phillips attorney or a member of our Data Security and Workplace Privacy Practice Group.

Related People



Benjamin M. Ebbink
Partner
916.210.0400
Email