Phishing, Spear Phishing, and Whaling: Protect Yourself and Your Law Firm

Law firms are major targets for cyber hackers. They recognize that law firm servers can contain extremely valuable data, from bank and medical records to business trade secrets and even classified government documents. Hackers want access to this information, so they take great strides to get it.

Some small and solo legal practitioners mistakenly believe that they are small enough to stay below the radar of cyber attackers. This simply is not true though. According to one ABA article, small and midsize firms are even more desirable targets for hackers. They know that these smaller practices have budget limitations that may preclude them from implementing adequate infrastructure and staff training for the prevention of cyber attacks.

While cyber attacks can come in various forms, there are some strategies that tend to get used more often than others. Phishing, spear phishing, and whaling are three types of social engineering attacks used to steal secure data. Let's look at how these tactics work and what you can do to protect yourself and your legal practice.

Phishing

Phishing refers to cyber attack attempts that target a broad audience by tricking people into sharing personal data. Attackers disguise themselves as trusted sources and send emails asking for specific information. For example, the attacker may send an email disguised as the victim's internet provider, requesting bank account information for a billing problem. The

recipient, believing that the email is legitimate, provides their bank account number to the attacker who then uses that information for personal and financial gain. Phishing can take the form of emails, text messages, and even social media with the purpose of stealing information from as many victims as possible.

Spear phishing

Spear phishing takes a more specific approach, targeting a particular individual or organization. In these scenarios, an attacker may pretend to be a family member or other person known to the victim. These types of attacks may take longer to implement because attackers work to appear as legitimate as possible, creating false letterhead, signatures, and addresses in their communications. Some common spear phishing examples include:

- An email from a business partner asking for payment of an attached invoice, which is actually just malware.
- An emergency situation requiring an immediate transfer of funds.
- A security alert appearing to come from within the organization, calling for the victim to change his or her password.
- A message from the company's HR department, requesting personal information for payroll or W-2 purposes.

Spear phishing is often used as the first step in a more elaborate cyberattack. Attackers use the information gained through spear phishing to launch a more sophisticated and widespread attack.

Whaling

Whaling takes phishing to another level by targeting high-profile victims. A play on words, "whaling" refers to targeting "the big fish" within a company or organization. Some examples may include politicians, CEOs, or celebrities. It uses spear phishing strategies to collect large amounts of data at one time.

Protecting your law firm

When working to protect your law firm from phishing attacks, there are a number of steps you can take to lessen your vulnerability. But your law firm members and staff are always your first line of defense. Human error is a major contributor to the vast number of cyber attacks that occur each year. If your employees cannot recognize suspicious emails or messages, they may unknowingly hand over confidential data to hackers.

According to a 2017 report, 82% of employees open email attachments that appear to be from a familiar contact. This is why it is extremely important to properly and consistently train your staff on identifying potential threats and handling them correctly. Give them the tools to recognize subtle warning signs, and what steps to take in response to data requests.

For example, firm members can make it a routine habit to check and recheck email addresses of suspicious emails. Maybe the sender's name is accurate in the message but spelled wrong in the email. Another possibility could be a few letters switched around or left out an email address or domain name. These may seem like small discrepancies. But taking a few minutes to double check can prevent a big data breach.

Another tactic your employees can use is the "hover and review" method. Unbeknownst to most email users, if you hover your mouse over the sender's email address before opening the email, the sender's full email address will appear. That way, instead of blindly opening a potentially dangerous email, you can first check to make sure that it is from a legitimate source.

These are just a few examples that demonstrate how proper training can go a long way to protecting your practice against phishing tactics.

Security measures

Now that you have your staff fully trained, it's time to make sure your internal security measures are up to the task of keeping you and your firm protected. Whether you are starting from scratch or working to improve the measures you already have in place, here are some strategies that experts recommend for keeping the hackers away.

- Email filters – Law firms receive tons of emails every single day. With an email filter in place, each of these messages will be scanned and approved (or denied) before entering your network. This tactic lessens the likelihood of phishing emails ever reaching your staff members.
- Up-to-date malware and anti-virus programs – These programs can be extremely useful in the prevention of cyber attacks, but only if they are kept updated. Cyber attacks are constantly changing, and an old malware protection program is probably not equipped to handle the most recent threats.
- Password policies – Require all firm members to use strong passwords and change them regularly. A weak password is like an open door to a hacker.
- Multi-factor authorization – Using a smartphone or another device, this authentication works to ensure that anyone trying to access your systems or email is properly authorized to do so.

Keeping your law firm safe from cyber attacks is your duty. Stay up-to-date on the latest threats and security trends, or at least contract with a vendor who can do it for you. For instance, TimeSolv legal billing and time tracking offers state of the art security measures to minimize the risk from even the most sophisticated threats. Their professionals consistently work to stay up-to-date on these ever-changing risks for you. To learn more about their services, click here for a free 30-day trial.

Whether you are concerned about phishing, spear phishing, or whaling, make sure you have measures in place to protect you and your firm.

About Erika Winston:

Erika Winston is a freelance writer with a passion for law. Through her business, The Legal Writing Studio, she helps legal professionals deliver effective written messages. Erika is a regular contributor to TimeSolv and a variety of other publications.