CYBER SAFETY

Keep your law firm safe and cyber secure*

Law firms play a crucial role for wealthy clients and commercial partners, often handling critical and sensitive data, and assisting in business transactions. As a lawyer, you may have access to intellectual property, merger and acquisition transactions—including contact information of deal team participants—and other confidential and personal information. Because of information and potential access available, hackers and fraudsters actively target law firms and other trusted advisors. A breach by a hacker can result in reputational risk, financial loss, compromise of non-public merger and acquisition transactions and exposure of contact information that hackers can use to facilitate sophisticated phishing campaigns and potential malware attacks.

As law firms and their employees have a professional responsibility to keep their clients' data and information safe from fraud, this piece is intended to help with cybersecurity safety procedures and best practices each lawyer and law firm employee can implement.

Cybercriminals employ a variety of methods to start a cyber attack and defraud lawyers and their clients, as demonstrated in the examples below:

Social engineering via email phishing	A partner at a law firm received a non-malicious email notifying him that he was to be profiled in a well-known business publication, and to expect a second email with a draft of the article. The second email contained a malicious attachment which, when opened, infected the computer system of the firm with a virus. The hackers were able to access key information about the law firm's clients and transactions.
Email spoofing	Cybercriminals registered domain names that closely resembled a company's legitimate domain name with the difference being a single altered letter or character. (For example, criminals might register "wibgetcompany.com" to target the legitimate domain "widgetcompany.com.") Cybercriminals then sent a fraudulent, or "spoofed," email to employees at the target company to individuals responsible for making payments. By not looking closely at the sender email, the company employees inadvertently sent out financial information to the cybercriminals.
Change in payment instructions	An attorney received an email that appeared to come from a client's employee, which informed the attorney that the client's banking information had changed. The email provided new remittance account information, and without first verbally verifying the change in account information, the attorney authorized a wire transfer payment to the new account. The account was in fact controlled by criminals who had hacked into the client's email account, and had sent the email to the attorney posing as the client.
Malware	After clicking on a malicious pop-up ad, an employee inadvertently downloaded malware that gave criminals access to his company's network and the user's credentials. Pop-up instructions on the screen asked the user to have a co-worker log into the same computer. When the co-worker logged in, the criminals used both sets of user credentials and were able to release a wire payment to their account.

*This document is provided for educational and informational purposes only and is not intended, nor should it be relied upon, to address every aspect of the subject discussed herein. The information provided in this document is intended to help clients protect themselves from cyber fraud. It does not provide a comprehensive listing of all types of cyber fraud activities and it does not identify all types of cybersecurity best practices. You, your company or organization is responsible for determining how to best protect itself against cyber fraud activities and for selecting the cybersecurity best practices that are most appropriate to your needs. Any reproduction, retransmission, dissemination or other unauthorized use of this document or the information contained herein by any person or entity is strictly prohibited.

CYBER SAFETY

Keep your law firm safe and cyber secure*

Protecting your firm's and clients' confidential information should always be a top priority. While your law firm may deploy sophisticated fraud prevention strategies, you are a critical component in preventing fraudulent activity. To improve your and your firm's cybersecurity posture and mitigate risk, our cybersecurity and fraud experts recommend taking certain precautions:

1. Avoid social engineering attempts

Not opening emails, clicking links, allowing someone to remote into your computer or downloading files sent by strangers will go a long way in protecting your firm. Cybercriminals may attempt to trick you into replying to or clicking a link in an email that may appear to be legitimate. Hackers take advantage of our trust and natural willingness to be helpful by employing social engineering techniques to break our usual cybersecurity practices, so it's important to learn how to recognize red flags. Additionally, ensure your firm has adequate email filtering in place to identify and block spam and other email-based threats.

2. Limit social media usage

Social media can be your biggest asset in marketing your or your law firm's capabilities. However, social media can also be a significant weakness if used incorrectly. Fraudsters can build up a profile of you or your firm and obtain information to socially engineer you or your colleagues into taking actions that can assist in schemes to defraud or harm you or your firm. Recommend that your firm enact a social media policy that provides appropriate guidance on social media usage by employees, and puts in place limits to personal webmail (e.g., Gmail, Yahoo, Hotmail) and other websites on company-issued devices.

3. Use strong passwords for email accounts, user accounts, systems and applications

Change your email account password at least every 90 days, if your firm doesn't already require you to do so, and make sure you use a strong password that uses a combination of upper- and lowercase letters, numbers and special characters. Passwords for systems, user accounts and key applications should also be changed frequently.

4. Use a secure email solution to communicate with clients

Ensure you are using a secure email solution for communication with clients so that sensitive information, such as financial transactions, intellectual property, wills, etc., are encrypted. Email encryption protects sensitive messages and provides the ability to encrypt the body of a message, as well as any attachments included, so that only authorized individuals can read the email.

5. Adopt secure processes when performing transactions online

When performing any online transactions, such as case registrations, briefing submissions or deal support, ensure that you have a unique user ID and you are not sharing login credentials with others. Never respond to pop-ups or unsolicited requests asking you to submit or resubmit your login information. If a website or login screen seems suspicious, log off and report the suspicious behavior.

6. **Be wary of emails containing wire payment instructions**
   Before you make or authorize any payment, verify the authenticity of the request by telephone. Use a telephone number known to you or available from an independent source, not a number contained in the email. Requests for payments to overseas bank accounts or any late changes to expected wire instructions should be especially scrutinized and validated. Recommend to your clients that they do the same by verbally validating any payment instructions.

7. **Implement multi-factor authentication whenever possible for online transactions and operational processes**
   Multi-factor, or two-factor, authentication is one of the strongest cybersecurity measures available and adds an extra layer of protection from cybercriminals. Types of authentication factors include: something you know (e.g., a username and password), something you have (e.g., a one-time password), or something unique to you (e.g., a fingerprint). Two-factor authentication is available from most email providers and online banking, finance, e-commerce and social media sites.

8. **Enable anti-virus and ad-blocking software**
   Ensure your firm has anti-virus software installed on firm servers, computers, laptops, tablets and mobile phones, with automatic updates to remove malware and viruses that could compromise your firm's email and network. Consider suggesting ad-blocking software, as malware is increasingly being served through online advertisements.

9. **Review your third-party vendors**
   Review and evaluate the processes of your third-party vendors. Hackers always target the weakest and most vulnerable link in the chain of business processes. Ensure vendors you work with have strong security policies and procedures.

10. **Cyber and fraud prevention education**
    Educate your team and colleagues about threats in the cybersecurity landscape and steps they can take to mitigate risk; protecting your business from cyberattacks is fundamental.

J.P. Morgan will never:

– Ask you to log in to the same computer with more than one user's credentials

– Ask you to repeatedly submit login credentials

– Contact you about online problems, such as logging in, if you haven't contacted us first

If you believe you have been targeted by a fraud scheme or your login credentials have been compromised, please contact your J.P. Morgan team member.

*This document is provided for educational and informational purposes only and is not intended, nor should it be relied upon, to address every aspect of the subject discussed herein. The information provided in this document is intended to help clients protect themselves from cyber fraud. It does not provide a comprehensive listing of all types of cyber fraud activities and it does not identify all types of cybersecurity best practices. You, your company or organization is responsible for determining how to best protect itself against cyber fraud activities and for selecting the cybersecurity best practices that are most appropriate to your needs. Any reproduction, retransmission, dissemination or other unauthorized use of this document or the information contained herein by any person or entity is strictly prohibited.