Keeping Data and Client Funds Secure

Atlantic Capital®

Guardians at the Gate - Keeping Data and Client Funds Secure

"There must be some kinda of way outta here, said the Joker to the Thief. There's too much confusion here, I can't get no relief...." - Jimi Hendrix

After a year of data breach after data breach dominating the headlines, many consumers are understandably concerned about the security and privacy of their personal data. According to a November 2018 Gallup poll, more than 70% of Americans worry about computer hackers accessing their personal, credit card or financial information. Unfortunately, consumers are right to worry - cybercrime is on the rise. In fact, the Internet Crime Complaint Center reports that consumers lost more than $1.42 billion to cybercrimes in 2017 - a 6.8% increase from the previous year.

An Industry Based on Trust

The Payroll / HCM industry has a unique place of trust with consumers, stewards of employee's funds and most sensitive information. Unfortunately, this trust is under attack from fraudsters and hackers intent to harm you and your client relationships.

Protect Yourself From Cybercrime

While the statistics above may seem daunting, you aren't defenseless against cybercriminals. Taking proper precautions is critical for protecting your client's sensitive information online. Here are some important protections you should consider to help safeguard your data and client funds.

1. When in doubt, verify

Criminals are getting more and more sophisticated, and they often use social engineering to trick victims into thinking fraudulent requests for information or funds are the real deal. Email phishing scams are one of the most common ways criminals attempt to access personal data. Read emails - even those from known senders - carefully. If something seems suspicious, give the sender and your primary client contact a phone call to verify the message is legitimate. Red flags include emails that are poorly formatted or use bad grammar, have an overt sense of urgency, emails that request personal data and emails that request additions/changes to payrolls that are out of sync with normal payroll cycles.

2. Double-check email address domains

Don't just look at a sender's name on an email; take time to review the actual email address and domain. Fraudsters can easily spoof an email address, turning bill.smith@atlcapbank.com into bill.smith@at1capbank.com, for example, and trick you into thinking you are corresponding with someone you know rather than a hacker.

3. Be wary of email attachments and links

Never open an attachment or click on a link within an email from an unknown sender. One of the simplest ways for hackers to gain access to your data or network is by tricking you into downloading an attachment or clicking on a link. Phony attachments can infect your computer with malicious software, so use extreme caution before opening. Hover over a link before clicking on it to review the full URL, or

continued...

Keeping Data and Client Funds Secure

continued

Atlantic Capital®

open a new browser and manually type in the URL to avoid being redirected to a criminal site.

4· Setup Dual Control Verification Procedures

Call the primary point of contact at your client to verify changes or additions to payrolls. Especially if it's a 1099 request and/or funds are being distributed to a payroll card instead of a standard bank account. Making non-verified changes to payrolls over email is the type of activity that fraudsters exploit. Do not fall into their trap.

5· Communicate with your clients about security / verification processes

Set expectations with your clients about security processes and verification of payroll changes. Let your client know you/your team will call to verify changes. Additionally, make your clients aware of cybersecurity best practices. In many recent fraud cases we have seen, your client's email has been hacked and the fraudster is communicating with the payroll firm as if he/she was your client through a hacked email domain.

6. Keep your systems and software up-to-date

Always stay current with the latest operating system, browser, anti-virus and other critical software updates. These updates can help protect against system vulnerabilities and keep bad actors at bay.

7· Train your teams & test for compliance

Our teams our always focused on serving the client. Fraudsters are typically trying to exploit this client first mentality. Make sure your teams are aware of the importance and sensitivity of their job as stewards of client funds and client data. Consistently review procedures around payroll changes / additions. Ensure your teams are not putting a client at risk by clicking on an unknown link or making changes to payroll via email.

We hope that these protections are helpful to maintain the trust and integrity of your client relationships. As always we welcome your thoughts and comments.