CyberPay Payroll Security

Understand and Prepare for Internet Crimes Targeting Payroll Providers

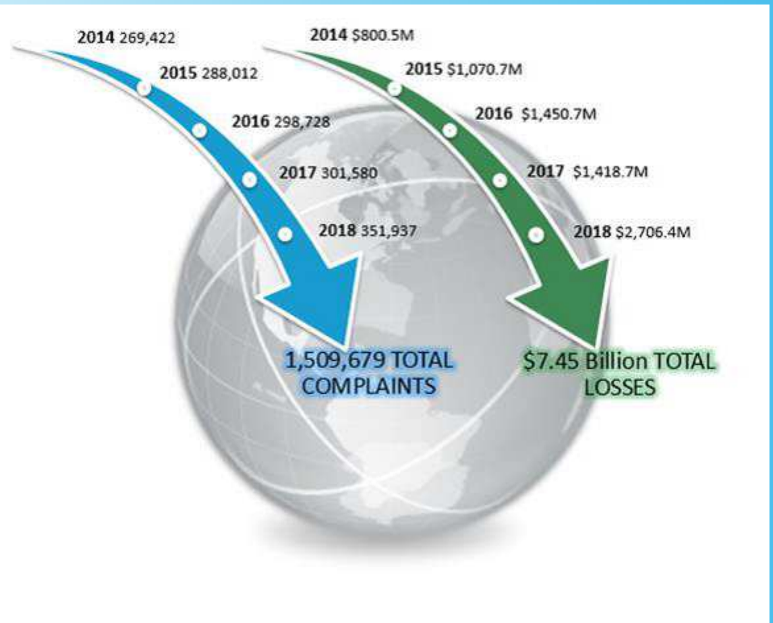
What you can do to lessen your vulnerability to payroll fraud and internet crime

sales@cyberpay.com || www.cyberpay.com || 866-231-3870

The Rise of Payroll Fraud

In 2018, The FBI's Internet Crime Complaint Center (IC3) received over 350,000 reported scams with financial losses of more than $2.7 billion. Business Email Compromise (BEC) more than doubled, accounting for $1.2 billion, nearly half of all reports.

Payroll is an attractive target because it circumvents many of the safeguards in place and since the payoffs are smaller, they're a lower priority.



FBI IC3 2018 Internet Crime Report Image includes yearly and aggregate data for complaints and losses over the years 2014 to 2018. Over that time period, IC3 received a total of 1,509,679 complaints, and a total loss of $7.45 billion.

-

The FBI also warns that tech support scams are increasing, with a 160% increase in losses last year. These scams prey on victims who are unaware that the fraudster is seeking access to their computer to install malware to gain banking credentials.

The Standard Email Scam

One scam is known as a Business Email Compromise or BEC. The fraudster sets up a Gmail or other generic account using the name of a company executive and simply asks that their direct deposit account be changed for the next payroll. It works, in part, because the emails are very well written and typically come from an executive, who many times can provide a voided check upon request. This urgent approach helps avoid the standard procedures for detection.

- Use Multi-Factor Authentication for employee self-service platforms.
- Rely on human interaction to verify the details; don't use email, pick up the phone.
- Secure social media so it's not obvious when you're out of town and unreachable by office staff.
- Watch for similar strategies, such as vendor impersonation requesting an urgent wire payment.
- Implement email security measures to monitor email conventions and look for "reply addresses" different than the "from address".
- Validate new direct deposit information by sending an ACH pre-note to the financial institution and issuing a live check for the first payroll after change is made.
- Set up alerts or reports on activities that could be associated with fraud, such as new hires, address or banking information changes, pay rate changes, multiple changes using the same routing information, employees using multiple direct deposit accounts.

The Imposter

Another popular scam is to impersonate an employer who needs payroll service. The fraudster will email or complete an online form requesting payroll. The alleged business is often brand new, a weekly payer and always pressed for time. They often use correct payroll terminology making it difficult to discern the legitimacy of the request.

Learn to recognize the hallmarks of a fraudulent request:

Request is urgent; rushing circumvents existing safeguards.

Payroll is weekly and they must begin this week.

Requires use all pay cards for employee payouts.

Employees often live in different states across the country.

Business is often in a different state than the payroll provider they are requesting services from.

Bank account to be used for payroll is often personal instead of business.

Salaries may be quite high for weekly payroll.

Develop processes to address them:

- Capture the IP address on their request and do a reverse lookup to reveal any mismatch in location.
- Always fund the first payroll from their account in order to do a pre-note to verify funds are truly from the account given to you in request.
- Rely on human interaction to verify the details; don't use email, pick up the phone.

If you receive one of the scam emails, you can report it to the FBI's Internet Crime Complaint Center.

Tax Time Provides Opportunity

IBM recognized an uptick in a Trojan virus, Trickbot, this tax season. Trickbot is delivered again via a professionally worded request from an email address spoofing a legitimate payroll business; once the addressee opens the attachment, the malware will be downloaded and can steal remote desktop and banking credentials during internet sessions from this computer and others on the same networks. The malware targets both personal and business email addresses.

- Secure all devices and applications with passwords.
- Keep all systems updated and patched per the provider.
- Don't open emails or attachments or enable attachment macros from unknown senders; consider disabling macros by default in Office documents. Use care with these files from known senders.
- Never enter log in credentials into a site from an email link or attachment. Go to your bookmarked sites.
- Use updated antivirus tools specifically to combat Trojans such as TrickBot.
- Instruct your customers to call you if they receive a suspicious email that appears to be from you.
- Search for existing signs of intrusion in your network.

If you receive one of these emails, you can learn more and report it to the IRS here or email it to phishing@irs.gov

The IRS communicates only through the US Postal Service and does not contact individuals by email or phone.

Monitor Your ACH Transactions

Each ACH originator has a unique identifying number. Some banks offer an ACH filter that allows debits only from preauthorized originators or in preauthorized dollar amounts. If your bank doesn't offer such an option, consider having accounts exclusively for authorized ACH.

Because the ACH system is comprised of largely unfamiliar groups and individuals, ACH fraud is difficult to detect and prevent. Bad actors need only a checking account number and a bank routing number to commit fraud and they use BEC phishing and malware scams to obtain that information. Tips for Prevention:

- Verify that you're dealing with the correct person; don't assume any unknown party is honest and confirm with known parties that they are requesting a transaction.
- Use your financial institution's fraud detection and prevention controls, for example, the aforementioned ACH blocks.
- Consider having separate ACH account by type, debit vs credit or for larger amounts.
- Remove ACH authorization capabilities when an employee leaves.
- Use encryption for emails.
- Add monitoring of these accounts to your daily processes.

You can learn more about ongoing schemes and prevention tips at the FBI's ICC website.

More than Just Payroll

Payroll is a lucrative target for obvious reasons, but the threat of internet crime is constant and the vulnerabilities are numerous. Consider the following as company policies and practices:

- Implement a Written Information Security Plan (WISP); all employees are required to agree and adhere to the numerous security measures in the WISP.
- Store any back-ups off-site.
- Block any websites that are not work related, such as personal email, social media, gambling, shopping, etc.
- Install and utilize a trusted Anti-Virus application that can protect you against viruses as well as email attachments that frequently can contain viruses.
- Perform regular browser history audits on internal computers.
- Use Enterprise firewalls that include an Intrusion Prevention System (IPS) feature if possible.
- Backup your data on at least a daily basis and then store the backups in a secure location offsite.
- Password protect your software applications using strong passwords, changing them regularly, particularly when an employee leaves your company.
- Invest in regularly scheduled third party security audits, including ACH specific audits.
- Employ or contract someone who understands cyber security and best practices.