Volume #4 - Issue #179
September 28th, 2018

This is a weekly publication dedicated to your personal cyber security. Our newsletter is designed to help the public recognize and avoid cyber threats while they are online. If you are not a subscriber, please go to HomeCyberDefense.net to sign up.

Protect Your Direct-Deposit Paycheck

Hackers are now out to reroute the direct deposit of your paycheck into accounts controlled by the cyber crooks. So, take a little extra time to verify that your paycheck hit your bank account, and beware of any official-looking emails related to company surveys.

According to the latest alert from the FBI, cybercriminals have been targeting online payroll accounts at school districts, universities, hospitals and commercial airway transportation. Yet scammers have been known to target all types of businesses using all types of payroll providers, according to a report last year in PYMTS.com. In some cases, employers discover the payroll-related scam only when employees start complaining that they did not receive their money via direct deposit. The FBI reportedly has observed an increase of such scams. In 2017, the FBI and the Internet Crime Complaint Center identified about 17 payroll-related scam cases. As of July, though, about 47 payroll diversion cases — with losses totaling $1 million — had been reported.

The scam starts out with a phishing email that aims to trick someone into handing over an employee's login credentials. Scammers will use social engineering to make emails look real, and they might appear to come from an address similar to a legitimate company account. Sometimes, according to payroll experts, this phishing email may request that an employee answer a brief survey and hit "confirm." The problem is that the employee is then directed to enter their credentials in an online form to confirm their identity. Authorities also noted that in some cases, cyber crooks might pick up the phone to call the employee resource hotline, provide the employee ID number and the last four digits of the Social Security number to reset a password, as part of the process to redirect the direct deposit.

The credentials can then be used to access the employee's payroll account in order to change the direct deposit. The crooks typically have that money directly deposited onto prepaid cards. The crooks then use the prepaid bank cards to receive cash withdrawals from ATM machines. Or they may make purchases at gas stations, grocery stores, retail stores, fast food restaurants and wireless phone carrier providers.

The FBI is warning employers to alert their staff about such schemes. Employees should not supply log-in credentials or personally identifying information in response to any email.

Some other tips:

- Log-in credentials used for payroll should be different from those used for other purposes, such as employee surveys.
- Companies should be on the lookout for employee log-ins that take place outside of normal business hours.
- Employers should direct employees to forward any suspicious requests for personal information to the information technology or human resources department.

Keep an eye on all your direct deposits and do not give your credentials to ANYONE by email without direct confirmation the request.

Thank you for subscribing to our email!