Fewer Mailed Checks and an Increase in Check Fraud

For the most part, people think of cybersecurity as only pertaining to digital hacks into networks, ransomware attacks where systems are shut down, or someone being spammed through email, etc. However, there is a physical component to cybersecurity that is as important as network security. An example is check fraud. As expected in this digital age, the use of checks has declined. The Federal Reserve of Atlanta, in their 2019 Federal Reserve Payments Study (FRS 2019), "found that the number of check payments in the United States declined at an annual rate of 7.2 percent a year from 2015 to 2018. In 2000, there were 42.6 billion check payments; in 2018, there were 14.5 billion, or about one-third as many." However, despite the decline in the use of checks, the fraud associated with stealing checks has dramatically increased. The US Treasury Financial Crimes Enforcement Network (FinCEN) reported that check fraud has increased substantially since the COVID pandemic. In 2021, the number of bank-filed Suspicious Activity Reports related to check fraud was over 350,000, a 23 percent increase over 2020. In 2022, the number of reported instances of check fraud was over 680,000; it had doubled. So despite the reduction in the number of checks sent through the mail, the US Postal Inspectors recover $ 1 billion a year in counterfeit checks and money orders.

What happens is simply the mail is stolen from someone’s residential or personal mailbox or a US Postal mailbox. The mail often proves a gold mine of personal identifying information (PII), credit card information, sometimes tax information, and of course checks. The criminals then use this personal information for identity theft; it is used to set up fake banking accounts or get a fake ID. The PII information is also used for follow-on cyberattacks, email scams, and the submission of fake credit card applications. Often, they will mail the IRS a change of address notification to get the refund check. The stolen checks are washed with an acetone solution, something as simple as nail polish remover. The goal is to remove the typed or handwritten payment information. Meaning the check amount is changed and increased, the “Pay to the Order Of” is changed to a fake business or person, and the signature is forged. The banking information remains untouched; the routing, account number, and personal information are all left alone. The checks are cashed with the fake IDs or deposited into the fake accounts, and after a short period, the accounts are closed. The money is spent before the victim is aware of what happened.

What has contributed to this in part is the use of Internet banking. Whereas before, checks were cashed or deposited at a bank, they are now deposited by phone, through a picture of the check, or at an ATM machine. The volume of these transactions has increased, and the validation of checks has declined due to volume and automation. The check payee is left unaware of the fraud until they realize their account is overdrawn. Then, the process begins with the bank and account holder sorting this out. This takes time, and the criminal is one step ahead.

There are a number of things you can do to reduce the risk of this type of fraud. Obviously, reduce the number of checks sent by mail. Another action is to clear out your mailbox. Do not let mail accumulate in your mailbox; though 60 percent is junk mail, it is the other 40 percent that is valuable to you and the criminals. If you are going to be away, have the post office hold your mail or arrange for someone to pick it up. Another thing is to ensure there is a lock on the mailbox; the old unlocked rural mailbox is a thing of the past.

The paradoxical thing is that as the internet and the sophistication of banking applications have grown to make banking more convenient and simpler for the consumer, it has also done so for the criminals. The banks end up paying for these losses, most of the time, and they are working to improve the security and integrity of these financial transactions. The US Postal Service is also working to combat check fraud, as they, too, must ensure the integrity of the mail service. However, the brunt of the effort to reduce mail theft and check fraud is with the consumer. Again, like your activity on the internet, blind trust will lead to an unpleasant ending. Reducing the checks you mail and receive is the best way to reduce risk. Safeguarding your mailbox as you do any external network device is another action. Another action is to monitor your credit cards and your bank accounts; prompt action if you suspect an illegal transaction increases your chance of stopping it and recovery. Consider eliminating old accounts or freezing credit cards. These actions are elements of physical and media security, focused on document security. These considerations are important to your business and personal life, as is access security to a network. Nevertheless, if you suspect you are a victim of mail theft related check fraud, like any incident, you need to act quickly to contain the damage. The first step would be to contact the banking institutions and get them involved. Of course, cutting through that bureaucracy may be easier said than done. Another recommendation is to contact the US Postal Inspection Service https://www.uspis.gov/report; (877) 876-2455.