The Latest News On ATM Attacks

cyber security risk management ATM

Summary: Because of the increased security of EMV chip cards, robbers are turning away from bank card theft and moving directly to ATM theft. What your bank should know.

The political scene has certainly become very toxic. We aren't going to ruin your morning by plunging into it, but we did find a recent survey on the subject quite interesting. A Pew Research survey found a whopping 68% of Americans surveyed said the news media favors one side when covering political and social issues; the same percentage lacked confidence that news organizations would be willing to acknowledge any mistakes made.

No matter the news going on around us, as bankers, it is part of our job to stay on top of the latest ways criminals try to steal money. Because of the increased security of EMV chip cards, crooks are turning away from bank card theft and moving directly to ATM theft. We have updated you a bit on this here before, but we wanted to provide you with more specifics to keep you up-to-date and aware.

ATM jackpotting, where thieves install malicious software or hardware into an ATM causing it to gush money, all started in Europe. According to the European Association for Secure Transactions, jackpotting attacks rose 231% in 2017 and attracted the attention of hackers in America.

The first attack in the US was in January of this year. This attack strategy, also called Black Box, begins with the attachment of a device to an ATM. It hijacks the control systems, modifies account balances and suppresses withdrawal limits. The criminals also implant malware in ATMs, often called Ploutus D, which then commands the machine to dispense all of its cash.

Another way to steal from a bank's ATM is as "a man in the middle". Here, malware intercepts the authorization approval sent from central command to the ATM and approves bigger withdrawals. Older standalone ATMs are high risk, so be careful.

To stay out of harm's way, community banks should be sure to intensify inspections of ATMs, perform regular risk assessments of the entire network, deploy hard disk encryption solutions and take other actions. Having alerts of any abnormal activity and a limited number of employees who have access to ATM systems can also help keep your machines out of trouble.

In some cases though, this is not enough. Hackers are already experimenting with another method of ATM theft called "ATM cash-out". In August, a bank in India lost $13.5mm this way. The crook broke in via a phishing email that was opened by a bank employee. Once the infrastructure became compromised, large foreign withdrawals were authorized and thousands of fraudulent transactions, including $11.5mm in unlawful ATM withdrawals, across 28 countries went unnoticed.

To make it difficult for hackers, the FBI recommends a few common sense measures. First, train employees to spot attacks across email servers or on social media accounts. Next, run mock attacks to locate the most vulnerable employees, and then retrain them. Third, step up security with two factor authentication for local administrators, by auditing administrator accounts, and checking encrypted traffic in unusual regions.

Also, of note: nearly all "ATM cash-out" robberies happen on the weekend, after the bank has closed. So, extra measures may be in order before heading out of the office.

WEBINAR: LEVERAGED LENDING

GETTING COMFORTABLE WITH A LOAN

OCT 10 | 10:00AM PT | Registration

Join us for a 30-minute webinar where we introduce you to one of the loans on our Shared National Credit Pipeline. Could this loan be the answer to your loan growth needs?