Feature Article

Cybercrooks Use Multiple Channels to Take Over One Bank Account

Sophisticated Cross-Channel Fraud Can Crack Tough Bank Security

Customers can access their bank accounts through many channels. They can go into their bank personally, use the web through a PC, call a customer service center or launch a mobile app. Fortunately, most banks are confident in their ability to secure each individual channel.

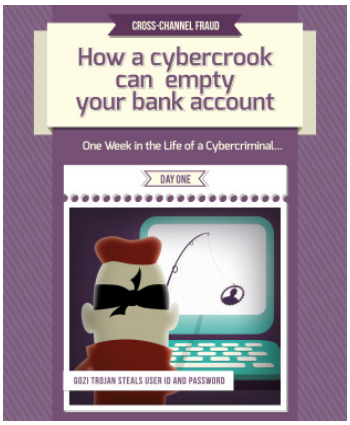
However, banks are much less confident in their ability to detect fraud when a cybercriminal enters from multiple channels.

Here's why:

- Different backend systems serve each channel
- Data is not usually shared between channels
- When cybercriminals use online channels only to gather information, the activity is typically not recorded
- If a security breach occurs, forensic research focuses only on the point of failure, not the interactions leading up to it

In an effort to accommodate customer demands for speed and convenience, banks rely heavily on information technology capabilities where automated processes use rules to validate a person's identity and approve a transaction. If a cybercriminal successfully penetrates one channel, the smart thief can then navigate through other channels without setting off any security alarms. Once a thief has assumed the persona of the target, they are able to provide account login and security information at each step that the closed system perceives as genuine.

Cross-channel fraud is one of the most common techniques cybercriminals use to take over a bank account ("account takeover"). When successful, a bank account is emptied and the money is simply gone. This is an example of how cross-channel fraud operates:



See Infographic

Feature Article

In this example, the thief first used malware to steal a user's credentials, then logged in from a different environment and, finally, leveraged a second channel – a call center.

Cross-session fraud, where a cybercrook uses the same channel for multiple activities, is a variant of cross-channel fraud. The same is true of social engineering attacks, where people are unwittingly leveraged or manipulated by fraudsters or hackers. Here is a good example of a cross-session, social engineering attack perpetrated on European banks where malware (a Ramnit Trojan) injected very convincing, interactive and real-time messages into a customer's web banking session:

1. Malware avoids detection by going into idle sleep mode until its intended victim logs into their online bank account
2. Malware activates and presents a fraudulent phishing message
3. Malware variants present the victim with new input fields, security warnings and customized text during login, account navigation and transactions
4. While the victim is reading the messages, the Ramnit connects to its command and control server and obtains the details of a designated money laundering bank account
5. A wire transfer is initiated

Clearly, cross-channel fraud has changed the cybercrime battleground, forcing banks to take a look at their online fraud strategies from a different perspective.

Now, the best way to catch a thief perpetrating a cross-channel fraud theft is to take a high level look at their behavior as they interact across channels.

Andreas Baumhof, CTO of ThreatMetrix – provider of security that protects against online fraud that includes account takeover, said: "As fraud patterns get more sophisticated and cross more organizational silos, banks need to invest in integrated analytics as well as traditional channel security."

Banks are starting to take cross-channel fraud seriously and are looking at ways to fight it head on. At the top of their list is implementing a common platform that identifies both trusted users and potential threats across multiple channels – the web, mobile web, applications, call center and onsite. With a 360° view of customer interactions, suspicious behavior is much easier to spot.

Cross-channel fraud is usually made possible because a smart cybercrook is able to go way beyond the theft of an account number, password and pin code. They use social media, web browsing and research within the target's bank account history to completely assume their victim's identity. They understand how traditional security systems work and prepare themselves to be able to breach every security layer in every channel.

So one key way to stop cross-channel fraud is for a bank to have a more complete profile of their customer than a cybercrook could possibly obtain. This requires understanding their customer's online behavior over time, where they are likely to be located, what device(s) they use and what activities they normally execute. Thanks to advanced technologies and powerful global data repositories, this information is now available to banks in real-time. If someone logs in from an unknown device or exhibits unusual online behavior, they can be immediately spotted and flagged for further review.

Feature Article

Another tool to block cross-channel fraud is malware detection. Technologies now exist that spot malware, enabling banks to block transactions or online activity from infected devices. Banks can also alert their customers about the problem, and use other ways to authenticate trusted customers so they can still complete transactions.

With global intelligence networks tracking billions of web transactions, cybercriminals have little room to manoeuver. Their digital footprints are either a matter of record or easily detected. By integrating this intelligence across all channels and blocking malware-infected devices, banks can go a long way toward stopping cross-channel fraud.

Media Contact

Lynn Strand
Director of International Marketing
Email: lstrand@threatmetrix.com
Skype: lynnstrand

For more information, please visit us at:
www.threatmetrix.com