The Latest Cyber Threats For Bankers

cyber security risk management

Summary: According to McAfee Labs, data breaches rose 20%, in Q3 2018 vs. the same period in the prior year in the financial sector. What should you expect from cybercriminals in the future?

Competition is always on the mind of community bankers. One new area to monitor in this area perhaps surfaced in some research by Bain late last year. It found 29% of those surveyed say they trust at least 1 technology company more than their primary bank and 54% said they trust at least 1 tech company more than banks in general. Clearly, this shows keeping customer loyalty is tough these days.

Another tough area where banks are focusing efforts is in and around all things cyber. As digital efforts have expanded in the industry, banks have significantly boosted security measures to thwart cybercriminals.

To see how things are going here, we look at data from the December McAfee Labs Threats Report. It found financial sector data breaches rose 20%, in Q3 2018 vs. the same period in the prior year. Specifically, McAfee researchers noted an uptick in spam campaigns using uncommon file types, namely IQY files (an Excel format), in an attempt to bypass email protection systems. These campaigns encouraged users to click on emails by using conventional social engineering phrases, such as "photos sent" and "please confirm." These operations accounted for roughly 500k emails sent globally.

McAfee researchers also observed banking malware intended to evade two-factor authentication. Here, malware was updated with slight modifications. One well-known hacking group, for example, has reportedly begun distributing a new version of malware that can give criminals remote desktop access in order to swipe information from banks, retailers and other businesses.

While these findings are troubling, they serve as an important reminder to banks to keep vigilant and try to predict future vulnerabilities even as we learn from past attacks.

This issue is addressed in a separate report by McAfee highlighting areas of potential future exposure. Notably, the security company expects cybercriminals to work more in tandem this year, creating more powerful threats in areas such as mobile malware, botnets, banking fraud and bypassing two-factor authentication security.

In addition, McAfee warned about artificial intelligence (AI) being used as a weapon in future attacks. Criminals have already demonstrated they can bypass AI engines and the next wave could be to use AI in malicious software. This would significantly up the ante for all banks, but especially for community banks.

Certainly, these disconcerting developments accentuate the importance of staying up-to-date on security, implementing upgrades and seeking professional help in thwarting attacks. For its part, the Federal Financial Institutions Examination Council recently released an extensive guide of cybersecurity awareness resources and statements for financial institutions to help.

This precarious situation also highlights the importance of ongoing training for employees to recognize suspicious emails and how to react in the event of a suspected security breach.

We've said before that cybersecurity is an ongoing fight, and the latest data underscores the need for continued vigilance. Banks can't afford to let their guard down as this battle rages on.