Collaborate with Customers to Help Prevent Corporate Account Takeover

With corporate account takeover (CATO) on the rise, commercial customers' lack of computer protocol and security is an increasing concern for banks. CATO is when thieves use malicious software to hack into a customer's computer, log into their bank's website and steal money and/or sensitive information.

If a customer is without adequate internal controls on their computer, a hacker can obtain control of it – and the customer's bank account – by simply searching the internet. After realizing their account has been hacked, customers may assume the bank is at fault for a lack of security. However, the bank is typically not to blame. For example, if the transfer request comes from a customer's authorized computer, there may be no way for a bank to detect a fraudulent transfer.

Banks can help protect themselves by encouraging customers to use proper computer protocol and internal safety procedures.

Establish/Confirm a Written Agreement

A written agreement with the customer establishes the criteria for transactions between the bank and the customer. By setting the rules and responsibilities in advance (including "Hold Harmless" wording), the bank can limit its exposure, while at the same time remind the customer that they hold responsibility for the security of their own systems.

Banks should also partner with customers in establishing safeguards on their account to help identify and prevent unauthorized access to their funds. Urge customers to implement a strong security program that includes educating employees about warning signs and proper responses to a suspected takeover.

Secure the Cyber Environment

Commercial customers should maintain proper systems and procedures to safeguard their cyber environment, such as encrypting sensitive data, using a protected internet connection and performing virus program updates. Customers should avoid using social media sites, personal email sites and online shopping sites on their work computers.

A growing trend for security-sensitive customers is to utilize a separate computer solely to conduct banking transactions. By limiting usage to banking transactions, disabling USB portals and CD drives, the customer can dramatically reduce the amount of exposure associated with CATO. Given the low cost of laptops, a dedicated computer has become a viable alternative.

Invest in Insurance

Stolen funds spark most CATO-related disputes between banks and customers, and customers without insurance often look to a bank to reconcile the situation.

Many banks are now requesting certificates of insurance from their larger customers confirming that they have coverage protecting their assets from CATO.

Conclusion

The most effective way to prevent corporate account takeover is for banks to share the responsibility with their customers. Banks can take an active role in ensuring appropriate security measures are in place by developing and maintaining a strong, collaborative relationship with customers.

About OneBeacon Financial Services

OneBeacon Financial Services offers property and casualty coverages for commercial banks, savings banks and savings and loan institutions, security brokers-dealers, investment advisors, insurance companies and credit unions. Specialty coverages, including management liability, professional liability, cyber liability and financial institution bond, are additionally available for institutions witl less than $3 billion in assets.

For information about our products and services, as well as tips and insights, please visit our website at onebeaconfs.com.

Contact Us

To learn more about how OneBeacon Financial Services can help you manage your unique risks, please contact Craig Collins, President, at ccollins@onebeacon.com or 952.852.2434.