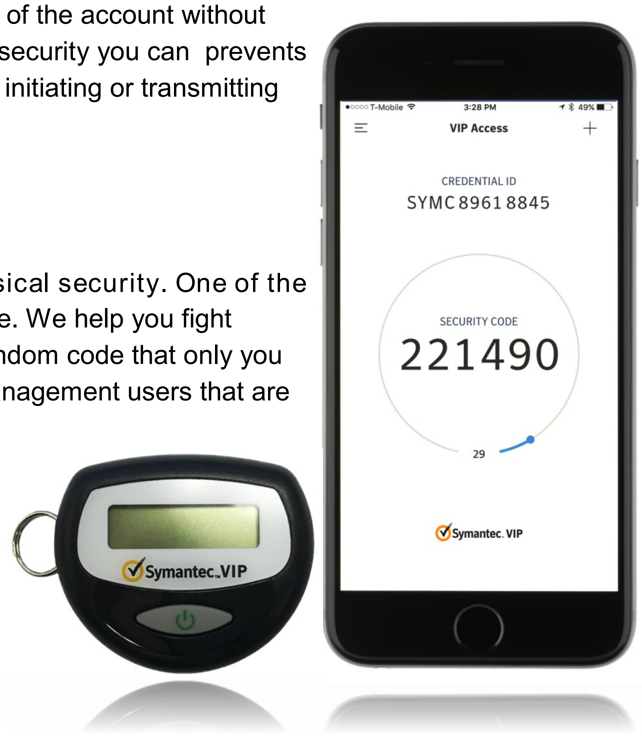
Your Security is our Priority

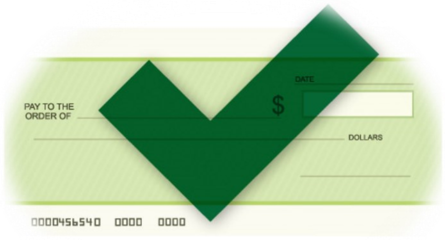
We know how important security is to all of our clients. Attacks on business systems can be particularly costly. In an age where most losses occur online by cyber crimes, we're investing in a security infrastructure that will help keep your business "safe at first". Because protecting your finances is our main priority we provide the highest levels of security, encryption and firewalls. And we haven't stopped there! We've added additional options that you can choose from as additional security layers to protect your assets even further.

Dual Control Access: One of the most common scenarios when companies lose money online is because there is someone having full control of the system with privileges that allow for money to be transferred out of the account without dual control. With our online layered security you can prevents a single user from creating, and then initiating or transmitting an ACH batch or wire transfer.

Security Codes: Avoid " man in the middle" attacks with physical security. One of the popular tactics of cyber criminals is injecting a key logger malware. We help you fight against this type of threat with physical tokens that generate a random code that only you have control and access to. We provide tokens to all the cash management users that are added to the online banking so that everyone logs in with these tokens. You also have the option to create or generate this code with a downloadable app that is available for iPhone and Android. Based on time synchronization technology, this authentication device solution generates a simple, one-time authentication code that changes at the push of a button.



Multi Factor Authentication (MFA) Security Questions: In addition to our already robust layers of security features we provide security questions which provide a strong out of wallet security that only the true user can identify and answer. These questions present themselves during initial login and whenever a high risk transaction is detected.



Positive Pay (Check Fraud Protection): For businesses that are check intensive we offer a way to fight against possible check washer and fraudulent endorsements. With PosPay you are able to upload a file directly from your accounts payable software to our online banking portal which will cross-reference against all checks that are issued and catch anomalies when checks are presented for cashing or deposit. The customer works these exceptions on a daily basis.

ACH Positive Pay: As more and more businesses are moving to electronic methods there are more chances for criminals to strike online. Our ACH PosPay system works with filters that are placed on certain debits that are allowed to pass through. All other debits coming through the account that do not match will be marked as an exception for attention by our client.

Feb 2017

Time Restrict: With time restrict you can set the time that you and your designated users can access the online system. This added layer of security prevents anyone from logging into online banking at times that the business may be closed. System flexibility allows you to set different access schedules for different users. If a user attempts to access outside of the allowable days/times, they are presented with a customized message indicating that they cannot log on.

IP Restrict: Take security to the next level with IP Restrict. This allows you to enter only specific IP addresses belonging to the computers at your business. This will prevent anyone with an IP outside of the internal network from access the online banking portal. With this option you designate it based on each user specifically. If a user attempts to log on and the IP Address does not match one on their trusted and enabled list, they are presented with your customized message indicating that they cannot log on.

eSAT Training: eSAT defines security controls to protect information in all forms, whether paper, digital, or verbal. This training helps every employee develop a clear understanding of social engineering, pretext calling methods, cyber threats, clean desk policies, standards for shredding documents, responding to an attempted breach of security, and ID theft prevention concepts and procedures. eSAT also includes instructional steps employees can use to educate account holders on how to avoid spyware, protect their non-public, confidential information from identity theft, and other preventative security measures. This interactive online training program offers question/ answer sessions throughout each session to ensure employee comprehension. Once the final assessment is passed, each employee receives a certificate of completion.

Empowering employees with specific knowledge about how to effectively secure non-public information and help prevent ID theft builds employee and account holder confidence while enhancing policies and procedures that keep your business secure and compliant.

Additional Information to consider

In addition to all of the aforementioned recommendations, it is more important than ever to have strong internal business processes within your company. When it comes to electronic transactions, be sure that your business uses dual controls internally, knows normal behavior of your customers, and performs prudent confirmation of your customer transaction requests.

Industry security experts also recommend use of a stand-alone computer to perform cash management activities. Ensure that the computer is hardened, is not used for web-surfing or email, and that anti-virus and security patches are installed and kept current.

We work hard to ensure that your accounts are "Safe at First!". For more information or to enroll in these enhanced security options, please contact our Treasury Services Professionals at 305-667-5511.

Feb 2017