Trustmark

SECURITY WATCH NEWSLETTER

Vol. 6, Number 2

Keeping Your Mobile Payments Secure

By 2019, worldwide mobile payments are predicted to surpass $1 trillion dollars*. Mobile wallet technologies allow you to store your payment information — a credit card or debit card number — inside an app on your phone and use your phone to make payments. Some examples are Apple Pay, Android Pay and Google Wallet.

A bank or payment card issuer can employ security features on its own payment or banking app, but it can't control the security features of third-party browsers where many customers manage their online accounts.

Despite advancements in technology, mobile payment protections are still in its infancy and aren't totally immune to intrusions by hackers and identity thieves. When you use a smart phone for wireless payment transactions, you are dealing with several kinds of technology that must all work together in a seamless but secure way.

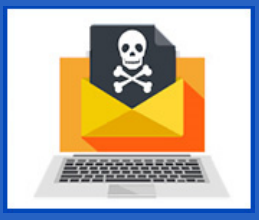
What you can do to protect yourself:

- **Only use a safe, trusted payment platform**, preferably the software that came with your phone. Reputable mobile payment platforms don't store your actual credit card details.
- **Device auto-lock and two-factor authentication.** Never disable the built-in security features, such as the screen locking capability on your phone that can prevent a phone thief from gaining access to the personal and financial information you have stored. Losing your phone is like losing your credit card. Ensure you use two-factor authentication to unlock your phone; for example, use a PIN along with a biometric method like your fingerprint to unlock it.
- **Only download trusted apps.** Mobile malware is becoming more prevalent. Too many apps available in app stores could contain spyware or malware that's designed to capture your payment information and send it to hackers without you ever knowing.
- **Don't use public wi-fi to send sensitive information.** Public wi-fi is shared with other users, and your private information could be picked up when it broadcasts. While away from home, consider setting up a personal virtual private network (VPN) for your phone when sending confidential information.
- **Monitor your financial accounts.** Should your financial information get into the wrong hands through a breach of a business to whom you've made a payment, the thief can add your payment information to their own mobile device and use it to make payments. Check your payment card transactions often.

Technology will continue to improve and so will the security of payment apps, but in the meantime consumers should take the necessary precautions to make sure private information remains secure.

*Source: * http://info.kount.com/white-paper/mobile-payments-and-fraud-2017-report*

How to Safeguard Against Business Email Compromise (BEC)



Business email compromise is an epidemic that is reaching historic levels throughout the world. Trend Micro has reported that business email compromise (BEC) attacks are projected to exceed $9 billion in 2018.

BEC is a type of phishing scheme where the scammer impersonates a high-level executive and attempts to get an employee or customer to transfer money and/or sensitive data. The threat of BEC spans across all industries, from retail, to healthcare, to manufacturing, to financial institutions, to not-for-profits - no matter the size or geographic location.

Fraudsters pose as a person with whom you have gained trust, such as an executive of your company, a reputable vendor, an attorney, or government agency. They send a fake, urgent request instructing you to wire funds immediately to payment instructions they provide. Employees who fear upsetting management, don't have access to management, or believe they are receiving the request from management, are less likely to question suspicious activity and more likely to complete the request. Unfortunately, victims don't realize they were duped until it is too late.

Many businesses are still not thinking about how they can make their processes resilient in the face of abuse and fraud. Here are some ways you can protect your business:

- **Review your fraud health** to determine where you have gaps and what you can do to improve your controls. You can significantly reduce cybercriminals' ability to exploit gaps in your organization by implementing strict corporate security processes.
- **Upgrade your email security.** Detect spoofed email addresses automatically and avoid scams by employing email security solutions.
- **Confirm requests for funds transfers** by making it mandatory to always ask for a secondary signoff using a method such as a phone call to a phone number in your system, rather than email.
- **Educate your employees.** They need to be trained to identify false communications, report suspicious activity and therefore, avoid the risk of fraud. Employees who understand email scams are critical in protecting your financial assets.
- Have an **incident response process** ready should this occur within your organization.
- **Report any incident** immediately to law enforcement or file a complaint with the IC3.

Fraud doesn't need to happen to your company. Business email compromise scams pose a significant threat, endangering both individuals and organizations and causing substantial losses. Fortunately, there are ways to prevent and fight these scams by combining best practices and email security technology.