Mobile Wallets: How to Safeguard against an Evolving Hacker Threat

Lynn Price, IT Security Strategist, IBM

What would you do if your wallet was stolen? Anyone who has experienced the headache and frustration of canceling credit cards or reordering a driver's license will affirm the importance of knowing where your wallet is at all times, and being extra wary of having it pilfered by a pickpocket when wandering through large crowds, riding the subway, etc.

Our mobile wallets should be no different.

What's a Mobile Wallet, and Do I Have One?

The concept of a wallet that doesn't reside in your back pocket can seem foreign at first. But carrying cash and other forms of physical currency is a convention that's rapidly declining in popularity. Mobile wallets aren't a fixture of the distant future – they're very real, and heavily in use today.

If you've gotten your caffeine fix by using a smartphone at your local coffee shop, then you're a mobile wallet user. Paying credit cards, checking on the health of your checking account – all these everyday activities affirm that humans are a mobile species that takes full advantage of the scan-and-go culture.

But don't take my word for it. There's hard data to back up these assertions: More

than one in three shoppers made at least one purchase with their mobile devices in the past six months. During last year's holiday shopping season 18.4 percent of retail site traffic came from mobile devices, up from 10.75 percent in 2011 (that's a 71.4 percent increase).

The question then arises: What are the security risks associated with a quick scan of your smartphone? In an age where hackers launch full-fledged attacks on banks and other institutions in an effort to steal valuable IP, you may think that nobody's going to waste a second thought on a single individual.

Think again.

The Changing Mobile World

Mobile devices are the security perimeter of your personal enterprise. Think about protecting your device, your identity, and your transaction when paying the parking meter or the taxi driver, or buying holiday gifts with the latest mobile coupon. Smart users are aware these complex mobile modules add more risk and opportunity for the crooks to insert themselves and take control. Applications that encrypt mobile transactions is just one safe-guard savvy users can utilize.

Being risk-aware doesn't mean being a paranoid mobile shopper. Mobile devices are a hot target for vulnerabilities, but it's not all bad news: Reports indicate that by 2014, mobile computing will be more secure than traditional desktops. Some hackers do it for the Lulz, but most seek financial gain and will follow the scent of money. As mobile commerce skyrockets it's safe to expect cybercrime to follow hot on its heels.

Malware has evolved; it's no longer as obvious as a Nigerian prince requesting your bank account PIN so he can temporarily deposit his life savings. Mobile malware is a lot more insidious, so to secure your mobile wallet from phishing scams and malware campaigns, take the following basic steps:

- *Be picky about your apps*: Do a little research on applications before installing them. Only download apps from trusted enterprise app stores, and be sure to check what permissions the app requires. If the permissions seem beyond what the app should require, do not install it. For example, why would a recipe generator need to access your GPS information? If permissions sound suspicious, it could be a Trojan horse, carrying malicious code inside an attractive package.
- *Use caution on public Wi-Fi*: Wireless mediums are often inherently more difficult to secure. There are repercussions to consider when signing up to become a node on a Wi-Fi network, albeit temporarily. Casual eavesdropping and more nefarious forms of access are a very real danger. Try not to purchase things or access your email account while using a public Wi-Fi zone. These hotspots are targeted by hackers because they can provide direct access to your mobile device. Using your own network provider connection is much more secure.

Another option to consider is utilizing a Virtual Private Network (VPN) when on Wi-Fi hotspots. A VPN provides a private tunnel for your data to pass through as it traverses the network. There are several that are free or low cost on the commercial market.

- *Research any charitable text requests*: Unfortunately, many people try to take advantage of public goodwill. If you receive a text message from an organization or an anonymous sender asking for a donation to their honorable cause, take the time to research the party requesting your money. Phishing attacks can be easy to detect to the naked eye, but their more deceptive relatives, spear phishing attacks, are highly personalized and harder to detect by the average person.
- *Use caution when scanning those ubiquitous QR codes*: Infected QR codes are a relatively recent (and unwelcome) phenomenon. QR codes can contain a URL to download malware, which can then send SMS messages to a premium rate number. “Scan here to get 10 percent off your next order” could lead to a scam.

To clarify a bit, QR codes eventually translate to a link which can infect the user device with malware. This is done typically via a JavaScript which is loaded as the website comes up. Once the device is infected, it passes control over to the hacker. At this point, the hacker can alter the on-going transaction or simply steal credentials to be exploited later or sold. QR code creation is freely available simplifying the fraudulent Account Take Over (ATO) opportunity.

- *Investigate mobile shopping coupons*: Yes, we all love them, but if it sounds too good to be true… chances are, it probably is. Coupon deals sent via an SMS message can be just as fraudulent as credit card offers sent via snail mail. When mobile coupons are applied to customer loyalty cards, the customer’s account, and identity information can be compromised.

In general, a strong dose of education coupled with a healthy helping of common sense is the perfect recipe for a secure mobile wallet. BYOD adds yet another layer to the security puzzle. This growing trend simply means that your smartphone is connected to your employer’s network and can be used for business purposes. It’s an attractive option for businesses, who typically want to give employees the added convenience of using a personal device to work wherever, whenever.

In a BYOD scenario your phone is the perimeter for your personal finance digital presence but also your employer. This adds complexity in safeguarding both environments including the flow of data from within the business to the outside world. Consequently, it’s no longer just your data that’s at stake if someone breaches the perimeter defenses – enterprise-owned information is also at risk. So do your due diligence and don’t be the weakest link in your organization’s security chain.

Conclusion

It is imperative that we equip ourselves with the knowledge and resources that are necessary to combat hacker threats – this effort should not stop when the workday ends. Anyone who uses a smartphone, tablet, or other mobile device to make online purchases must maintain proper vigilance over their mobile wallet in the interest of ensuring that their personal and financial information doesn't fall into the wrong hands.

When the security of your mobile wallet is in doubt, reporting any suspected fraud is always a safe course of action. Being a good mobile citizen means relaying malicious schemes so that others don't fall victim.

Secure mobile data doesn't have to be an oxymoron – with the proper precautions, anyone can rest assured that their mobile wallet hasn't fallen into the wrong hands.

About the Author

Lynn Price has over 25 years' experience in the Information Technology arena with broad expertise in the IT application, networking and security domains. She has held many leadership and management positions advising IT Strategic Outsourcing clients in their overall IT and security management strategies and programs. She has focused expertise and deep insights in the financial sector. She is a currently a Security Strategist for the Financial Sector for IBM Security Systems. In that capacity she provides business collateral to external and internal clientele with leading trends, insights and best practices in a fast changing IT security world.

Source URL (retrieved on *11/28/2014 - 8:23am*):
http://www.wirelessdesignmag.com/blogs/2013/11/mobile-wallets-how-safeguard-against-evolving-hacker-threat?qt-blogs=0