Luxury Daily®

The News and Intelligence You Need on Luxury

COLUMNS

Key steps to secure the mobile wallet

June 24, 2013

By Lynn Price

Most of us do it every day – it is as simple as buying your morning coffee at the local coffee shop.

You place your order and then finalize the purchase with your smartphone. All it takes is one scan and you are quickly on your way.

Not only can you buy your coffee with your smartphone, you can pay your credit card bill and check the health of your checking and savings account.

If you take a moment to step back and look around, you realize we are a mobile species and there is no turning back.

Phony money
Mobile purchases make life easier and, besides, who actually ever has cash on them anyway?

Physical currency may eventually be an historical relic. Mobile purchases are the present and future.

According to a recent report from the e-tailing group, more than one in three shoppers made at least one purchase with their mobile devices during the past six months.

In addition, look at the stats from last year's holiday shopping season: 18.4 percent of

retail site traffic came from mobile devices, up from 10.75 percent in 2011, for a total increase of 71.4 percent.

Using your smartphone to make purchases is only going to increase, and soon it enough it will become your mobile wallet.

But do any of us really consider the security implications with that one quick scan of the smartphone?

In this day and age of security without boundaries, these smartphones are the new front line of cyber defense.

Educating ourselves is always a good start. It is more important than ever in the throes of a disappearing security perimeter, alongside a burgeoning growth of mobile devices.

There is no need to become a paranoid mobile shopper, but if you are at least risk-aware, you are security-aware.

In fact, some reports indicate that by 2014, mobile computing will be more secure than traditional desktops.

As more dollars move to mobile purchases, a hacker is potentially not far behind.

But there are steps you can take to protect your mobile purchases.

On the money

Here are a few recommendations on how to help better secure your mobile wallet from phishing scams and malware campaigns:

• *Choose apps carefully:* Do a little research on applications before installing any of them.

Only download apps from trusted enterprise app stores. Check what permissions the app requires.

If the permissions seem beyond what the app should require, do not install the app. It could be a Trojan horse, carrying malicious code in an attractive package.

• *Limit your activities while using public Wi-Fi:* Try not to purchase things or access email 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.

• *Research any charitable text requests:* Unfortunately, some folks out there will try and take advantage of your goodwill.

If you receive a text message from an organization or an anonymous sender asking for a donation to their honorable cause, please take the time to research the party requesting your money.

Phishing attacks can be easy to detect to the naked eye, such as the infamous Nigerian scams.

But spear phishing attacks, which are highly personalized, are becoming harder to detect by the average person.

• *Avoid recklessly scanning QR codes:* The first instance of infected QR codes occurred not too long ago.

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% off your next order" may lead to a scam.

• *Investigate mobile shopping coupons:* Yes, we all love them but just like the old saying goes, sometimes a deal is too good to be true.

Just like fake credit card offers you get via snail mail or in email, coupon deals sent via text message can be just as fraudulent.

EDUCATION SPRINKLED with a little common sense will not only protect you, but help you consider the implications if your smartphone is connected to your employer's network.

Consider the data as it flows from your phone, through the wire and to the outside world. All the data and information you have that is private as well as enterprise owned is now potentially at risk.

Extending these safe-guarding practices a step further, you should report any fraud immediately.

Be a good mobile citizen, so others may not have to go through the same experience. You never know, your action could lead to end of a particular phishing scheme.

In summary, the world is evolving quickly to an environment where smartphones are prolific and the traditional security perimeters are evaporating. It only makes sense to arm yourself with education and awareness.

Lynn Price is IT security specialist at IBM, Boulder, CO. Reach her at llprice@us.ibm.com.