Ready for the holidays? Maybe not?

You're building your shopping lists, checking your credit card balances and scanning for can't miss deals. You may have even installed new apps that can automatically scan and compare prices to make sure you are getting the best deal.
But what about cyber security? How safe are you when you are holiday shopping?
Here are some things to consider when you are out and about during holiday shopping season.

Safe shopping

· "We've been having trouble with that card reader all day." That may be true. It also may be because a skimmer has been placed on that reader that uses those extra card swipes to capture your data before letting you make your purchase. You might want go to another line or rethink your purchase.
· Look for signs of tampering. Are the colors or materials on the card device consistent? Are the graphics aligned? Are there gaps or seams between components? Do components line up exactly? Is there any damage around the card slot that might indicate that it was forcefully removed or replaced?
· Hide your PIN. Some skimmers have a pinhole camera located nearby to capture your PIN. They can be disguised as anything. Best practice is to cover the keypad with one hand while entering your PIN with the other.
· Compare devices. Does the device you are using look like the ones around it? Check colors, flashing lights, size of the device, materials used, etc.
· Wiggle everything. ATMs and credit card machines are designed to withstand thousands of users. They don't have loose parts or components. If the cover moves, the keypad is loose, the card slot wiggles or moves when you push on it or when you insert your card, or anything feels less than industrial grade, move on.
· Check to see if the tamper-proof tape on the credit card component placed on public ATMs is intact. Most will display a VOID message if they have been tampered with or removed.
· Use your credit card rather than your debit card as it provides you with fraud protection.
· Report what you find. Most ATMS have a phone number to report something suspicious, and cashiers and store managers need to be alerted. It's the holiday season – take a few minutes to help the next shopper in line.

NFC (near-field communications) risks

If you are using a contactless payment card or smartphone to pay for items, you should know that these devices use a technology called near-field communications that can be monitored and captured remotely. At holiday time shoppers can surround you. So if you are using a contactless payment system, look around you first, and insist that anyone standing right next to you move several feet away before you use your phone to make your purchase.

Cybercriminals will disable a chip reader or cause it to display an error, forcing you to swipe your card using your magnetic strip data. If a payment device has been enabled to read chips, but keeps giving you an error message, you may want to consider an alternate form of payment.

Track your bank and credit card statements

Look at your bank and credit card statements online during heavy shopping periods, rather than waiting for your statement to arrive in the mail weeks later. The quicker you spot unauthorized transactions the faster you can get the resolves and limit your exposure.

Don't leave stuff in your car

Even if it's locked in the trunk. Here's why. Electronic car key fobs that allow you to remotely lock and unlock your car, open the trunk, or even start it and run the heater or air conditioning are now standard issue.

Your key fob and your car's electronic security system both use algorithms to generate a random lock code. When the devices are synched together and you press on your fob, the numbers match and the car locks or unlocks itself. Unfortunately, these devices sometimes get out of synch. Manufacturers solve that problem by letting the devices store a rolling set of numbers, called a rolling code scheme, so that if the numbers don't match right away it can search for other codes looking for a match. It doesn't matter what you drive – with few exceptions, most manufacturers all pretty much use the same concept, and in certain cases, may be vulnerable to this type of attack. The same hack can be used to open a surprising number of garage doors and other electronic locks that use the same sort of rolling code scheme, and step-by-step instructions are likewise available online to enable cybercriminals of just about any skill level to take advantage of this vulnerability.

Connected devices

Many of the items being purchased this holiday season are devices that connect to the Internet for one reason or another. Unfortunately, few of these devices were designed with security in mind. These devices can often be used to collect personal information, or can be hijacked and used as weapons, such as a recent series of denial of service attacks that redirected traffic from tens of millions of compromised devices, such as digital cameras and DVRs, to shut down the online services of a targeted victim.

Vulnerable connected devices can include:

- Smart entertainment systems - game consoles, TVs, DVRs, DVD players, and online gaming
- Smart accessories – watches, phones, tablets, laptops, weather clocks, radios
- Smart toys – dolls and toys with corresponding online lives and data, remote controlled vehicles – including those that can be driven or flown using your smartphone, interactive toys that can be updated online
- Smart appliances – everything from toothbrushes to washing machines
- Smart cars – entertainment systems, communications, onboard computers and diagnostic systems, and automated payment systems for parking or fuel

Of course, hacking these devices themselves is not the problem. No one is really interested in hacking into your smartwatch to figure out your exercise routines, your calorie intake, or your weight loss plan. But they ARE using reconnaissance hacks to discover your passwords for the Wi-Fi network at work, or your account information for automatic online purchases, to steal or spoof your identity, or even to figure out when you are away from home.

Accountability

We all need to become more aware.

While there are standards established for the secure transmission and storage of credit card information required by the payment card industry, there are currently no legal requirements that the connected devices you buy are safe from cybercriminals. As consumers we need to insist that vendors take this challenge seriously. Many times, security standards are created only as a reaction to the fear of government-mandated regulation, or the loss of business.

And finally, we need to take the time to educate ourselves - and our friends and family – about how to shop carefully and safely.