INVESTIGATOR INSIGHT

Consumer Tips for the Holidays 2012

Protecting your identity during the holiday season

Keeping your sensitive information safe

It's once again the time of year when consumers are making plans to visit relatives, host festive get-togethers, and, of course, hit the stores (or computer) for some shopping. Unfortunately, the flurry of activity that goes hand-in-hand with the holidays presents a prime opportunity for a data thief to practice his trade. With that in mind, put the protection of sensitive personal information at the top of your holiday to-do list.

Kroll's Investigators offer the following tips that can help consumers keep their sensitive information safe:

Tip #1: Practice safe shopping in stores

- Before you hit the stores, take stock of what you bring along in your purse/wallet. Remove unnecessary key identity components. Make a list of what remains so you'll know what is missing if your purse/wallet is lost or stolen.
- Consider your preferred method of payment—each has pros and cons. Generally, from a theft standpoint, credit cards are safer because, unlike debit cards, you usually have more protection against fraudulent charges. Cash is another option, but while you will not have to worry about personal identifiers, it will be gone for good if stolen. Be very careful with checkbooks, as stolen checks can give the thief access to your checking account.
- Do not leave your purse/wallet in your vehicle. Many people do this and then find themselves a victim of theft of property and then theft of identity.

Tip #2: Practice safe shopping online

- Never use a public computer (like those found at the library) to perform online financial transactions. Likewise, if the coffee shop is offering free—yet unsecured—wi-fi, don't be tempted to use your computer to buy anything there either. You never know if a public computer contains some type of malware, and thieves can steal data via an unsecured wireless internet access.
- Protect your personal computer, tablet, and/or smart phone. Use security software and install updates as available.
- Visit only reputable retail sites. Be wary of deals appearing too good to be true as it may be an avenue for a thief to take your money or identity information.
- Just as you would keep receipts from the stores, keep a record of all your online transactions. Check your debit/credit accounts to make sure only the transactions you've authorized have been registered. If you see any unauthorized transactions, dispute them with your financial institution immediately.

Tip #3: Think before mailing holiday cards

- E-cards are convenient and fun, but beware: disreputable e-card websites may load malware on your computer and may send it along to all of the recipients as well. Send e-cards from a reputable source, and check the end-user agreements to ensure that no software will be downloaded as a condition of using the service. If you're receiving the cards, beware of cards that have generic sender information, such as "a friend" or "a relative." If the card comes with an attachment, particularly an executable (.exe) attachment, it's best to delete it.
- Snail mail is still a popular way to send greetings and gifts, particularly gift cards or checks. If you send a check, use a dark, pigmented ink that can't be easily "washed." Washing is a process a thief uses to take away the ink on your check so it can be rewritten to them, with a higher dollar amount.
- Never leave mail with sensitive information in an unlocked mailbox—mail it from an official USPS mail drop box. For items that arrive at your home, you might consider purchasing a mailbox that locks.

Tip #4: Protect yourself and your guests at home for the holidays

- Secure any documentation in your home that may contain sensitive information, such as bank statements, checkbooks, credit cards, Social Security cards, etc. Keep these items in a locked cabinet, if possible, and in an area that will be inaccessible to guests.
- For your guests, assign a safe area to keep purses and other personal items. Make sure only one person is allowed to collect or retrieve these items.

Tip #5: Protect personal information while traveling

- Never leave sensitive information in your hotel room or car. If you wish to leave your laptop in the hotel, be sure to put it in your room safe. Or, consult hotel management to arrange for storage in a centralized main safe or secure holding area.

- Further, beware of pretexting, or social engineering calls, while staying at the hotel. This scam has become extremely popular, so much so that many hotels now post warnings to hotel guests not to provide their personal information, particularly credit card information, over the phone. The front desk already has this information on file and has no need to call you for it. If you do get a call, ask for the person's name and call the front desk yourself to verify.

Tip #6: Do not announce travel plans on social media websites

- Part of the fun of social media is being able to share your adventures. However, do not tell everyone when you will be away from home or post photos that reveal you are away. This is an invitation to property theft which can lead to identity theft. Share details of the trip after you return.