Toolbox Talks

Holiday Theft & Shopping Safety Part 1

HOLIDAY CRIME PREVENTION & SAFETY TIPS

Black Friday, kicking off the busy holiday shopping season, starts the highest theft time of the year. Phone theft, Pick Pocketing, & Purse snatching are always more common & significant during the holidays. These crimes can be classified as either a crime against property or a crime against person depending upon the circumstances involved during the commission of the offense. In the case of purse snatching, it can produce long term effects in the victim. The loss alone cannot be measured in just the financial loss of the purse, but there is the distrust in walking unharmed in public & in our own familiar surroundings. It's time consuming when you consider the notifications to various companies & organizations to replace important documents. Credit cards must be canceled, work identification replaced, drivers licenses duplicated, check books reordered, house keys & locks replaced, & old photographs of loved ones may be lost forever. The threat of Identity theft makes these losses even more traumatic. Additionally, with all our data & information saved on our phones these have become one of the top targets for theft. Behind the increase in crime: A lucrative market for used phones. Thieves can sell pilfered devices to local merchants or street-corner middlemen or hawk them on sites such as eBay.com, Amazon.com or Craigslist.org, where a used iPhone, for instance, can fetch several hundred dollars. **So if your phone or tablet is lost or stolen, report it IMMEDIATELY.**

Purse snatching is a crime that usually focuses on the elderly & citizens with one or more physical difficulties that would hinder their ability to fight back or give chase. The criminal depends on speed & the element of surprise to accomplish the act. Some purse snatchers prefer to attack from behind, knocking the victim to the ground. This is dangerous to the elderly or persons with a health disability. The thief will usually never keep the purse more than five minutes after the crime. An arrest with the purse in their possession is the kind of evidence the thief does not want. They will need only enough time to go through the purse to obtain cash & valuables that can be pawned. The purse is often discarded in a dumpster, storm drain, low roof, or over a fence into a yard. The purse, if recovered, will often be found anywhere from a block away to a mile from the scene of occurrence.

The following are suggestions offered to help reduce your chances of becoming a victim of this crime:

1. **Carry as little paper currency as possible.** Rely on credit cards &/or personal checks for large purchases. Credit cards & personal checks can be replaced, but money can't.

2. **Carry your keys in your hand**; **they make an excellent weapon to protect yourself**. Don't carry your keys or important medications in your purse. The loss will prevent you from driving, entering your home, reading necessary documents, or taking important medication for your health.

3. Beware, if you are knocked down & you chose to struggle for the purse, the criminal could become more determined & cause you extreme physical harm to accomplish the act.

4. When shopping, never leave your purse unattended. Never leave it on a restaurant seat, in shopping carts, public rest room floors, dressing rooms, or under your seat in theaters. Wrap the child restraint on a shopping cart around the purse handles to make it hard for the thief to grab & go.

5. **If your purse is stolen a&someone telephones to request you respond & get your purse, DON'T! Let the police pick it up. It could be the thief looking to rob you of more valuables.**

6. The target areas for pick pockets are back trouser pockets & suit coat & sports jacket pockets, located both inside & out. A pickpocket generally avoids front trouser pockets & especially buttoned or zippered pockets.

7. If you have to carry your wallet in an unbuttoned jacket, coat, or pants pocket, be sure it holds only what you can afford to lose. Keep money, credit cards, IDs, in your front pocket or any buttoned or zippered pocket. Some people even place a rubber band around their wallet, because the rubber band creates friction & rubs against the fabric of your pocket if someone is attempting to remove it without your knowledge.

8. Never pat your pocket to see if your wallet is there; this lets a criminal know the exact location of your valuables.

9. When driving in your car, keep your doors locked & keep the purse on the floor behind your seat. You don't need someone smashing your window & taking your purse from the front passenger seat.

10. Never keep pin numbers, account numbers, or any safe combination numbers in your purse, if you do, the thief could benefit from this information.

11. Always assume the purse snatcher or purse thief still has your house & car keys. Change locks immediately. It may save you a bigger loss in the future.

12. A purse snatcher can be anyone – a man, woman, or child. They are not the stereotypes television often portrays them to be.

13. Never leave your purse near your front door. A person knocking on your door could see the purse & force their way inside to get it.

14. Keep the purse flap closed & secure when in a crowded area. It will keep "sticky fingers" out.

15. **Purse theft can happen anytime, anyplace**. Constant vigilance is needed to deter criminals. Be ALERT & AWARE of your surroundings. Pay attention to who is around you & what activities are happening. Dont leave the safety of a building or your vehicle until you have ensured all is secure & safe. Trust your instincts; if you feel uncomfortable with a place or person(s), get away.

16. Park in well-lit areas, dont wander into risky areas alone or at night.

17. Keep a list, separate from your wallet, of contact numbers to report lost credit cards.

All information provided by the Clovis Police Dept. & Unisys Systems Safety Representatives found at nationalsafety.wordpress.com
Articles written by Ken Oswald

Toolbox Talks

Holiday Theft & Shopping Safety Part 2

Avoid Holiday Scams

As the holidays bring an increase in online shopping, charitable giving, & social interaction, consumers & businesses should be on guard against some common scams. The dangers of online fraud continue to grow.

The Top 10 most prevalent scams are listed below, along with tips on how to avoid them:

1. **Online shopping threats:** In the United States, the FBI reported that more than $250 million was lost in 2010 due to online fraud. To avoid being yet another victim, Unisys security experts recommend that online shoppers always shop on safe sites that have SSL (a protocol for secure communications) certification, indicated by a locked padlock at the bottom of the screen. If you have second thoughts about using a site or retailer, follow your instincts & avoid it. Where possible, use a credit card rather than a debit card as banks can often offer consumers a higher level of protection when a credit card is used. If buying through sites such as Amazon or eBay, take the time to read the seller feedback. Finally, be sure to check your bank statements regularly for any unexpected purchases.

2. **Seasonal spyware:** The number of malicious e-cards circulating to personal & business computers is expected to rise this year. Unisys experts suggest that even in a workplace setting, individuals never open an e-mail or attachment from an unknown sender & do not download exe files as these often contain adware, unwanted downloads, & spyware.
If you cant resist opening a file, drag it into your junk e-mail folder first as this allows you to check all the links to see if they are legitimate. If a site looks suspicious, follow your instincts & dont click on it. Finally, be sure to install personal firewall, anti-malware, & protection agent software on your computer. So if you make a mistake & click on a malicious e-card, you will have some protection.

3. **Not-so-social networking:** Enterprises & individuals are making increasing use of social networking sites such as Face book & Twitter to keep in touch with clients, partners, friends, & family over the holiday season. Unisys security experts warn that these sites can be a goldmine for identity thieves. According to GetSafeOnline, 1 in 4 people using social networking sites have posted confidential or personal information such as phone number, address, or e-mail on their online profile. To avoid identity theft, never offer personal information to anyone over a social networking site, even if the request is from a friend or relative. Do not offer your birth date, birth town, & home address on your user profile, & always make sure you apply the right privacy settings to protect yourself. Avoid posting photos of expensive belongings or dates when you are away from home over the holidays.

4. **Beware of ATM skimmers:** Whether at your neighborhood bank or at your office lobby or credit union, Unisys experts stress the importance of being aware of your environment when using an ATM to obtain holiday shopping cash. If you think someone is too close behind you or looking over your shoulder, find a different ATM.
Thieves are becoming more & more sophisticated, so also check the actual machine to make sure that it is solid & sturdy. Some skimming scams have involved fitting the front of an ATM with a false panel containing a small webcam or digital camera that can capture your card details. If the ATM appears to be behaving oddly or does not work the first time, go to a different machine — dont try it again.

5. **Fake Online Payment Sites:** Escrow services such as PayPal allow businesses & consumers to securely & conveniently send & receive payments online. However, escrow scams are increasing as fraudsters set up fake payment sites to con both buyers & sellers out of money.
To ensure payment sites are legitimate & secure, Unisys security experts suggest checking to ensure the sites have SSL certification. Also check that the web address starts as https:// rather than just http:// as the absence of that s is often an indicator of rogue traders. A real escrow company will also only ask you to transfer money to them directly from your bank, i.e. a traceable transfer. If they ask for another method, refuse. Before you send anything, verify with your bank where the receiving bank is located. If this looks like it is outside the seller's own country, stop the transaction.

6. **Spirit of giving scams:** Christmas is the season for sharing &, as a result, thieves will often make the most of peoples' generosity over the festive season. Unisys suggests that individuals watch out for e-mails or tweets from charities that ask for donations, particularly if you have never signed up to receive correspondence from them. Be sure to check that charity collectors in your neighborhood or near your office have some form of identification.

7. **Gift grabbers:** After opening all the presents, Unisys recommends breaking down the boxes completely so that what was in the box is not obvious to passersby on the street. Thieves are more likely to target homes with home theatre or PC boxes in the trash. The same is true of business-related or personal bills, receipts,& financial statements — all of which could contribute to identity theft. & as always, employees must protect their companys intellectual property by safely disposing of materials that are proprietary to their companies.

8. **Protect your new laptop:** If you receive a new PC or laptop running on MS Vista or Windows 7 as a holiday gift, Unisys suggests making sure you use anti-malware software & enable the firewall before connecting to the Internet. Whether you are connected to a wireless network or via a cable, on average, it can take just nine seconds for your new laptop to receive its first ping attack & less than a minute to receive its first virus.

9. **Free Wi-Fi & wireless network hacking**: If you are using that new laptop on a wireless network at home or workplace, Unisys recommends making sure that network is secure. This is because the Wi-Fi network range will radiate beyond the confines of your building, leaving it vulnerable to war driving (the act of searching for Wi-Fi wireless networks by a person in a moving vehicle, using a portable computer so they can use your unsecured network for free).
Hackers could use an unprotected wireless network to anonymously download illegal material or perpetrate attacks that would appear as if they were coming from you. War drivers are also known to hack into computers to steal personal details. In one highly publicized case, a retailer reportedly lost more than 45.7 million personal credit & debit card details to hackers. The crime went on for four years before it was detected.

10. **Account check & phishing cons:** Unisys security experts recommend that individuals at home or work be wary of account checking scams in which a phony representative of a bank or supplier who contacts you by phone or e-mail to ask for account details to update their records. Callers will often claim that they need certain data in order to check the security of your account while actually obtaining very valuable information to carry out fraud. In the lead-up to Christmas, remind your family, friends, & colleagues to err on the side of caution & refuse to give out any personal details either on the phone or online. If you think the call is genuine, ask to call them back & check the number by visiting their website before you call back. Likewise, dont assume that an e-mail that looks like it comes from your bank or a company you've done business with is legitimate. In common phishing attacks, e-mail messages from impostors contain links to phony look-a-like sites where your login ID & password can be captured. Always suspect that web links in unsolicited e-mails may be fraudulent, & dont provide any personal information to such sites.