



LYNNE ABRAHAM
DISTRICT ATTORNEY

**DISTRICT ATTORNEY'S OFFICE
THREE SOUTH PENN SQUARE
CORNER OF JUNIPER AND
SOUTH PENN SQUARE
PHILADELPHIA, PA 19107**

NEWS RELEASE

Date: Friday November 23, 2007
Contact: Cathie Abookire / 215-686-8711
Director of Communications

**DISTRICT ATTORNEY LYNNE ABRAHAM AND CHIEF INSPECTOR
ANTHONY DiLACQUA OUTLINE CONSUMER SCAMS AND SAFE
SHOPPING STRATEGIES**

- 1. Protect Yourself From Scams**
 - 2. Protect Your Identity**
 - 3. Protect Your Packages and Possessions**
-

WHAT: NEWS CONFERENCE

WHEN: BLACK FRIDAY
NOVEMBER 23, 2007
11AM

WHERE: DISTRICT ATTORNEY'S OFFICE
Three South Penn Square
Corner of Juniper and South Penn
Mezzanine Level

November 23, 2007---"Black Friday" marks the beginning of the busy holiday shopping season, and District Attorney Lynne Abraham and Chief Inspector Anthony DiLacqua remind everyone that it's a busy time of year for criminals as well as holiday shoppers.

"There is always somebody looking to separate you from your money," said District Attorney Lynne Abraham. "The best course of action is prevention."

"Many thieves choose their victims because the thieves see an opportunity," said Chief Inspector DiLacqua. "If you take away the opportunity, chances are you won't become a victim."

Online:

1. Use a credit card rather than a debit card for online shopping. Most credit cards cap your liability at \$50, whereas there may not be a cap with a debit card, which is an open invitation to your entire bank account.
2. Dedicate one credit card for online shopping only. It will be easy to keep track of purchases—and unauthorized purchases.
3. Your social security number is the key to your identity. **DO NOT** give out your social security number while shopping online.
4. Online shoppers must be vigilant in avoiding scams and protecting their personal information.
5. There are several holiday scams this year:
 - Name a Star—Very popular, there is no such thing. Only the International Astronomical Union names stars, and they are not selling names.
 - Fake Charities-- Reputable charities **DO NOT** solicit online.
 - Unsolicited Bulk e-mail solicitations---It is not worth the risk of opening yourself up to possible scam artists.
 - Instant credit offers
 - Free travel Vacations
6. Also beware of high pressure sales and online auctions. They may be legal, but you may overpay.

Other Popular Scams

- **Mortgage Aid Scams**---Scammers ask people to send them money directly, which may even result in victims losing their homes.
- **Nigerian Bank Scam**---Promises money if the victim will process a check, which of course is fraudulent, through the victim's account. Very popular to the tune of millions of dollars.
- **Lost Pet Scam**---Scammers find lost pet ads in the paper, contact the grieving pet owner and say that the pet was taken to Mexico. Owners call a bogus long-distance phone number to the tune of hundreds in phone calls, which goes straight to the scammer. The pet, of course, is never found.
- **Phishing**--fraudulent emails that prompt consumers to reveal social security numbers, bank account numbers and other 'keys to one's identity'—is expanding to include more businesses, including Citibank, Fleet, eBay, PayPal, and the FDIC. Consumers should also watch out for fake emails from charities.
- **Pharming** is another cyberscam that redirects users from a legitimate website to a fake website without their knowledge. Then, when the user types in a username and password, criminals capture the information. Consumers are advised to research antivirus software that addresses this scam.

“Nobody is safe from thieves or cyber crime,” said District Attorney Abraham. “If your identity is stolen, you could spend 18 months to three years in credit purgatory. Prevention is critical.”

On the ground:

Since thieves work on the ground as well as on the internet, the D.A. and the Commissioner offer the following strategies to avoid being a victim of crime:

1. Guard the chain of custody of your credit card. If you give your credit card to a clerk or restaurant server who then takes it in the back and swipes it on a ‘wedge,’ the information on the magnetic stripe from your credit card can be duplicated.
2. **Do not put your purse in a shopping cart.**
3. Keep your wallet in an inside pocket, and strap your purse around you and tuck it under your arm. Beware of people bumping into you or distracting your attention by engaging you in conversation. This is an old scam to divert your attention in order to steal your wallet or purse.
4. Place your packages in the trunk so they cannot be seen. Always park in a well-lighted area.
5. Do not park next to a van. Criminals can pull you into a van as you go to your car, and nobody will see it happen.
6. Always accompany young children to the restroom. Tell your children in advance to look for a source of help ***within the store or mall***, such as a uniformed police officer or a salesperson with a nametag.

On the Phone:

“Crimes of persuasion” are the schemes, scams, and frauds that con artists use to steal your savings. Watch out for sob stories, sweepstakes, lotteries, and wacky investments, secured credit card offers, credit repair offers and even fortune tellers. While some telemarketers are legitimate, do not give out social security numbers or credit card numbers to unknown people on the telephone.

Other Methods:

1. Accessing your credit report by posing as an employer, loan officer or landlord.
2. Stealing mail from mailboxes to obtain credit card statements, bank statements or other personal information.
3. Taking trash bags from the street with old credit card and bank statements
4. “Dumpster Diving” into trash bins to retrieve financial statements.
5. Motto: Shred, shred, shred, and be sure to use a **cross-cut shredder**. Vertical strips can easily be pieced together, and vertical shredders should be avoided.
6. Dishonest employees with access to your personnel records.
7. Misdirected mail or email with personal information.

Most Valuable Documents for Thieves:

1. Social Security Card—The ‘magic’ number. Do not carry your social security card with you, and do not give out the number. If you are asked for the number, ask the person what would happen if you didn’t give it out. In many cases, it’s not necessary.
2. Drivers license

3. Credit Cards
4. Telephone calling cards
5. Birth certificates
6. Passports

“It is often difficult to find the perpetrators of scams and online frauds as well those who would steal your wallet,” said D.A. Abraham and Chief Inspector DiLacqua. “Prevention is the key.”