El Paso County Sheriff's Office

Neighborhood News

A key to driving safety in the winter is to make sure your wiper blades are in good shape.

Inside this issue:

Evolving With Technology

In today's world, people must keep up with technology in order to conduct their daily routines. They are required to adapt daily to new knowledge and exciting discoveries that are constantly changing the way they live and do business. Today, everything from saying hello to a friend down the street to videoconferencing with someone around the world can be done electronically, from home.

Technological advances now allow people to carry out the most mundane of tasks, such as ordering groceries from the store, to the most complex activities, such as performing complicated surgery, all from a separate, remote location: a computer connected to the Internet.

Since its beginnings in the 1990s, the Internet has grown into a vast electronic network that now spans the entire globe, and it will only continue to grow. Because people use the Internet in their everyday lives, they rely on it for a safe and accurate exchange of information.

Constantly, personal data such as Social Security numbers, credit card numbers, and passwords are traveling through wires, and also through the air, from one computer to another. With security measures in place to protect this sort of information

online, most people feel safe on the Internet and trust that their personal information will remain confidential. But, unfortunately, criminals have also adapted to advancements in technology and, these days, people are becoming victims of crimes committed over the Internet.

The Evolution of Crime on the Internet

For years, criminals have been using discarded credit card receipts, bank statements, tax notices, and other bills (often found in the trash) to gain the personal information necessary to assume another person's identity. However, on today's electronic playing field, these criminals have used technology to devise cunning new methods of theft in the form of cyber crimes. Now, computer hacking and email scams known as phishing are included among the risks of sharing information online.

Computer hackers are able to enter areas of the Internet where they are prohibited and hack in to another computer network. Once they are inside a computer's network, they are able to view documents, files, and confidential data and use it for their own personal gain. Phishing, on the other hand, is a method in which people are duped into providing their own personal data to a thief who is posing as a legitimate business or agency. Both

of these cyber crimes have been steadily on the rise in recent years. In fact, according to the Wall Street Journal, there were more than 9.9 million cases of identity theft last year in the United States.
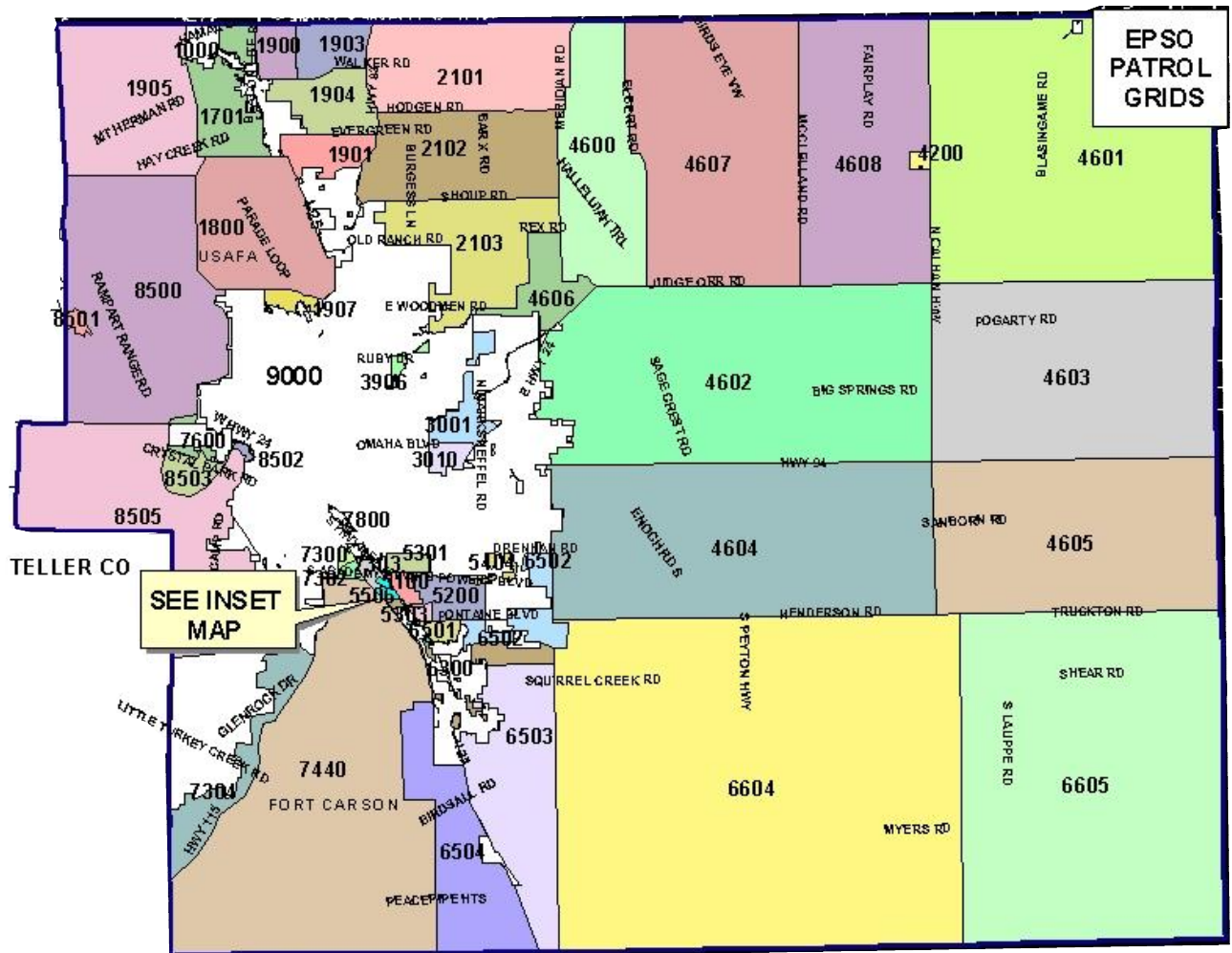
Hacking Into Your Life

One example of the growing computer hacking problem in which personal information was stolen emerged in February, 2005 when an information broker, ChoicePoint Inc., announced that an identity theft ring had hacked into its database and gained access to hundreds of thousands of personal documents. Some of the information that was stolen included full names, Social Security numbers, home addresses, and credit reports.

Many other large corporations such as T-Mobile USA were also recently hacked, and had their clients' information stolen. Even superstar Paris Hilton could not escape the threat of identity theft as her personal photos, text messages, and phone numbers in her personal directory were stolen by a hacker and spread across the Internet. The U.S. Senate will soon hold hearings to determine whether these corporations and information brokers require more extensive regulation.
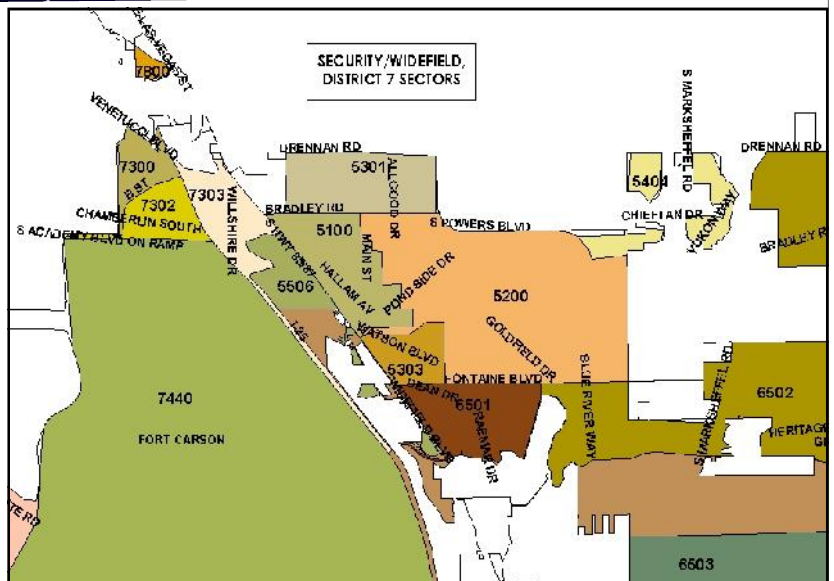
El Paso County Reporting Districts

(The first digit of the number shown on the map is the District number. For example, the area marked as "4602" is within District 4.)

El Paso County Sheriff's Office – Area Breakdown: For a more detailed breakdown of districts and crime statistics for your area, visit the following web page:
http://shr.elpasoco.com/crime_stats.asp

District 1 - Woodmoor, Gleneagle, Kings Deer, Club Villas
District 2 - Black Forest, Wissler Ranch, Hawk Ridge
District 3 - Cimarron Hills, Constitution Hills, Claremont Ranch
District 4 - Woodmen Hills, Falcon, areas east of Meridian Road
District 5 - Security, Fountain Valley, Colorado Centre
District 6 - Widefield and Little Ranches area
District 7 - Stratmoor Valley, Stratmoor Hills, B Street, SW Highway 115
District 8 - West Colorado Avenue and Ute Pass

Crime in Your Neighborhood: Highlights From November/December 2010

District 1: There were six burglaries and four cases of criminal mischief reported in District 1 during this time period. One vehicle was reported stolen. The vehicle owner stated that the garage door may have been left partially open and that the keys were taken from the counter inside the house. There were six cases of theft from vehicles. These incidents do not appear to be related. There were also two cases of criminal trespass during this time period.

District 2: There were eight burglaries during this time period. All were forced entry into a residence: four were through a garage door. Only one had a locked door from the garage into the home and burglars did not make entry into the home. In four cases, the burglar(s) gained access by kicking in an entry door to the home. There were three cases of criminal mischief - two of which were damaged mailboxes. Of five vehicles stolen in this district during this period, four were taken without permission by a party known to the owner. There was a single criminal trespass - a domestic related.

District 3: There were 31 residential burglaries during this time period - 18 were forced entry. In two of the non-forced entry incidents the burglar entered through an open or unlocked garage door and in three cases by using keys or garage door opener left in an unlocked vehicle in the driveway. There were 21 cases of Theft from vehicles - about half of the vehicles were unlocked, and most had valuables in plain sight within the vehicle. There were 11 vehicles stolen - three of them were left unlocked and running in the driveway.

District 4: There were 19 residential burglaries - only five were not forced entry - and 14 cases of criminal mischief during this time. There were six stolen vehicles, most from businesses, and 5 cases of theft from vehicles. There were ten drug-related cases - eight of them marijuana. Animal complaints were a combination of ownership of a dangerous dog (five cases) and animal cruelty/neglect (eight cases).

District 5:   There were 15 residential burglaries - nine were forced entry - and 26 criminal mischief cases occurred during this period. Three vehicles were stolen from this district, there was one attempted steal and four previously stolen vehicles were recovered. There were 22 cases of theft from vehicles - about half of them were unlocked. There were seven cases of criminal trespass.

District 6: There were six cases of residential burglaries - only one was forced entry. Of the others, two were entry through open/unlocked doors or windows and three were possibly by a person known to the victim. There were 24 cases of criminal mischief - eight of them vandalism to vehicles. Six vehicles were stolen in this district - two of them were unlocked and had keys in them. There were 11 thefts from vehicles - in three of them the vehicle was unlocked.

District 7: During this time period there 11 residential burglaries - in four of them suspects were arrested. There were 22 cases of criminal mischief, arrests were made in eleven of the cases. Eight vehicles were stolen and one previously stolen vehicle was recovered. There were 42 instances of theft from vehicles - ten of them occurred on 12/22 in the Sherwood/Denise/Maxwell. In the early morning hours there were reports of two males dressed in black looking into parked vehicles with flashlights. Several deputies responded to the calls, and contacted the owners of the vehicles which had been broken into. On the morning of 12/27, there was a similar rash of 12 break-ins on Forest Rd and Hartford St - not far from the break-ins of the 22nd. No arrests have been made for the break-ins.

District 8: During this time period, there were four burglaries - three of which were residential. One robbery occurred, and an arrest was made. There were four vehicle break-ins: all vehicles had been locked. There were also three drug cases - two of which were marijuana-related.

Crime Prevention Safety Tips

1. Have secure locks (deadbolts, screen door locks, window/door pins, sliding glass door locks/bars/dowels, etc) on all doors and windows including between your garage and house, and use them even when you are at home.
2. Do not leave your vehicle running unattended, and always remove your keys and garage door opener from your vehicle - even if parked in your garage.

Phishing - Don't Get Hooked!

Phishing is currently on the rise around the world as well. Phishing works because scammers are able to construct bogus emails, pop-up ads, and even websites that appear to be from legitimate businesses or agencies. They inspire a false sense of trust, then send out emails asking for personal and financial data so they can steal identities.

Some phishing emails may even install software on your computer that could be used to redirect your computer to bogus websites. Be extremely cautious of whom you trust with personal information on the Internet. You should know that legitimate businesses will never ask you to provide nor confirm any personal information through an email or pop-up message.

Tips to Protect Yourself and the Internet

FOR EMERGENCIES, DIAL 9-1-1

El Paso County Sheriff's Office Dispatch (non-emergency crime reporting): 390-5555

EPSO Telephone Reporting System (for minor crimes without suspect information): 520-7111 or http://shr.elpasoco.com — click on the icon "Online Reporting CopLogic"

EPSO Traffic Hotline (for reporting problem areas or traffic violations): 520-7192

EPSO Tip Line (for reporting suspicious activity or the location of wanted persons): 520-7777

The Internet can be a powerful tool, and the convenience it offers to manage business and recreation is invaluable. But theft and fraud are damaging the positive reputation of the Internet as a medium for business. Consumers are losing confidence in their own safety on the Internet, and fewer people are making purchases online these days.

However, there are steps that you can take to decrease your chances of becoming a victim, and to help catch cyber-criminals at work:

● Be aware that there are people online who would like to gain access to your personal information. Do not share this information unless you have initiated the exchange or are absolutely sure of who is receiving it.

● Install security and scanning software onto your computer to protect it from online hacking.

● Do not use your name, date of birth, address, or any other personal information for passwords. These passwords are easily cracked by hackers. In fact, it is suggested that for any password, you should not use a word that is found in the dictionary, as there are hacking programs that will attempt every word in the dictionary.

● Never disclose personal information in response to an email. Legitimate businesses would never ask you to do this. If an email or pop-up ad requests you to confirm personal information, even if it looks genuine, it is an example of phishing and should be reported to reportphishing@antiphishing.org, the attorneys at the Securities and Exchange Commission at enforcement@sec.gov, and to the Federal Trade Commission at uce@ftc.gov.

● If you are concerned about an email you receive from a company, contact that company by phone to verify the information. If there is a web link provided in the email, type it directly into your browser instead of using the link or copying and pasting it, as some links can be redirected to other sites.

● When giving personal information over a website, check to make sure that site is secure. Look at the first part of the web address in your browser. It should read https:// and not http://

● Regularly check your credit card and bank statements and keep track of your transactions. Also, log into your online accounts frequently. This way, you will be able to notice any changes to your account soon after it happens.

By taking these steps, you can greatly reduce your chance of having your identity stolen, and help to combat this growing problem. If you are careful not to reveal personal information online, and help to make others aware of the risks, you will be playing a part in making the Internet a safer place for all of us to communicate and conduct business.

For more information on phishing and identity theft visit the Anti-Phishing Work Group.

This article reproduced with permission from the National Crime Prevention Council website