FRAUD ALERT

Let the buyer be Aware!

www.scconsumer.gov Fall 2008 Volume 3, Issue 4

Lap-locked! How to protect your laptop from hackers, thieves, everything but coffee spills

A laptop computer defines convenience and mobility. It enables you to work from home, a hotel room, a conference hall, or a coffee shop.

Maybe you've taken steps to secure the data on your laptop: You install a firewall. You update your antivirus software. You protect your information with a strong password. You encrypt your data, and you're too smart to fall for those emails that ask for your personal information. But what about the laptop itself? A minor distraction is all it takes for your laptop to vanish. If it does, you may lose more than an expensive piece of hardware. The fact is, if your data protections aren't up to par, that sensitive and valuable information in your laptop may be a magnet for an identity thief.

Chances are you've heard stories about stolen laptops on

Continued on Page 5

Rip-off! Company pressures, threatens businesses to pay for OSHA posters

The South Carolina Department of Consumer Affairs (SCDCA) warns businesses not to fall for unsolicited telephone calls attempting to sell Occupational Safety and Health Administration (OSHA) posters or other state and federal government materials.

These deceitful companies use high pressure sales tactics and vague threats of fines and criminal charges to pressure businesses into purchasing government mandated materials at a cost of hundreds of dollars. Often the company will have an official sounding name and may reference being affiliated with various government programs, but they are not.

The truth is these materials are available free of charge. The posters can be acquired by contacting the U.S. Department

Continued on Page 6

Think before you click

E-mail phishing scam uses "YouTube" links

The South Carolina Department of Consumer Affairs, along with the SC State Library, are state agencies with modest budgets and have learned to use some alternative approaches to disseminate information and education. One such way is YouTube, a social media site that allows users to upload video content for others to view. SCDCA currently has several videos that enjoy a large audience not just in this state, but nationally and with viewers in some 20 foreign countries.

For more **information** on scams involving social networking websites see our **"Top 5 Scams"** article on **page 3**.

The accepted link to these spots is found on the Department's website, and that's where it will stay because scammers have found yet another way to compromise consumers by using something familiar and in the news. Online security experts are alerting net users to be wary of messages urging them to watch the latest viral video on YouTube.

They say it may be part of a scam that is sending out tainted links in order to ultimately break into computers and steal your personal information.

The present scam is founded on the habit of net users to casually click links forwarded to them by online acquaintances, not realizing that the

Continued on Page 5

Fraud in South Carolina

The following is a sampling of recent consumer reports of attempted scams or fraudulent activity in South Carolina. The Department handles hundreds of calls concerning possible frauds, scams, and other confidence schemes each month. Consumers are advised to be on the lookout for these scams and to stay vigilant.

Aiken – A woman reported that her father sent $100 to a group known as the "Secret Society" that promised to send back books and publications in return. The group has since asked for more money without sending any additional products.

Columbia – A woman received an unsolicited advertisement from a group that claimed in return for a $30 a month draft on her bank account they would fix or replace any large appliances in her home. The woman had never heard of the organizations and no public records were available. The company refused to accept checks, saying it would only honor bank drafts.

Columbia – A woman reported an unsolicited call to her place of business offering to sell smoke detectors and asking for credit card information.

Hartsville – A woman reported a strange incident in which her husband received an unsolicited phone call from a company promising him contractual construction work if he paid them $600.

Charleston – A man received an unsolicited phone call telling him if he did not press 1 or 2 on his telephone his credit would be ruined.

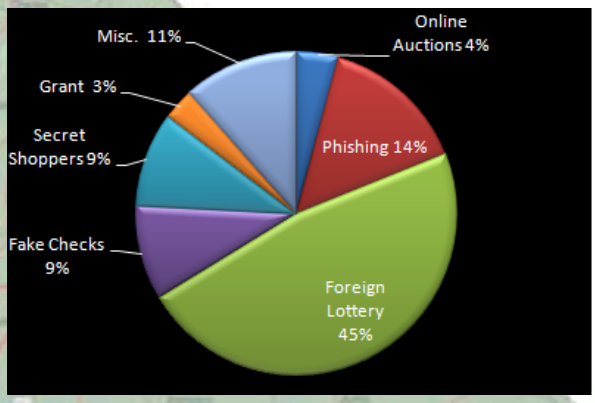
Columbia – A business reported that a group identifying itself as the Labor Law Compliance Institute telephoned them claiming they were in violation of OSHA regulations and needed to immediately purchase $140 in signs and posters or they would be fined. The group claimed to be with the government, though they were not. OSHA posters can be obtained at little or no cost from the government.

Gaffney – A man said he received an unsolicited phone call claiming if he gave over his bank account number he would be charged just $93 in return for lifetime protection against identity theft and fraud.

Greenwood – A bank reported that several elderly residents were being solicited to send in hundreds of dollars for the promise of thousands in return. There was no return on the money sent in.

If you suspect fraud call the Department of Consumer Affairs at 803.734.4200, or toll free, 1.800.922.1594. Postal fraud should be reported to the postal inspector at 803.733.4642.

What scams are going around?



The most popular frauds reported to the Department of Consumer Affairs are foreign lottery or sweepstakes scams.

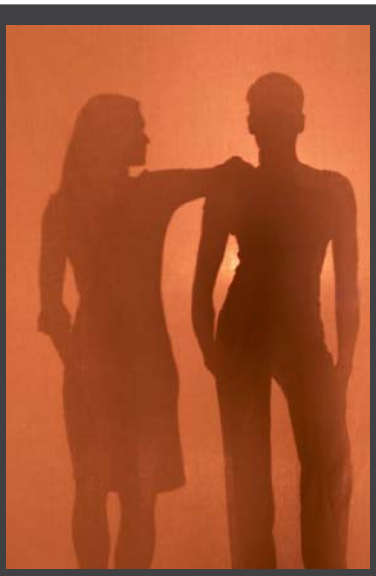
Typically, these scams involve receiving unsolicited mail with an enclosed check for several thousand dollars and a letter explaining that you are the lucky winner of a foreign lottery, shopping sweepstakes, or other contrived story. The scammer will then ask for you to deposit the check and wire back a large sum of the money as payment for taxes, filing fees, or other bogus charges.

The check is a fake – no matter how good it looks – and the scammer is hoping you wire the money back before the bank realizes their error.

Recent economic turmoil has many Americans looking for additional work and scammers are taking notice. Secret Shopper scams appear to be on the rise. There are legitimate secret shopper organizations, but unfortunately there are a lot more corrupt individuals who are looking to make a dishonest buck.

One of the telltale signs of a fraudulent secret shopper program is any request for you to wire money back to the organization.

Many of these scams involve a fake check they ask you to deposit, spend a small amount of on a particular product or store, and then wire the bulk of the money back. Honest secret shopper organizations do not operate this way.



5 SCAMS! to look out for on social networking sites

Internet security experts are increasingly concerned about the rapid growth of social networking scams.

Social networking sites such as Facebook, MySpace, Flickr, and LinkedIn offer users a chance to do anything from sharing music to making business contacts. It is estimated that more than 70 million people and organizations utilize at least one of these social networking communities and the number is growing.

Unfortunately, scammers are opportunists and the popularity of the medium combined with its relative recent emergence makes it fertile ground for scams, rip-offs, and frauds.

Social networks have become part of the fabric of online life and their popularity is likely to increase for many years to come. And there's no doubt they're a great way to make friends or do business. But, just like any other sort of platform that contains personal information, you have to be careful and use some common sense.

The following are the 5 most common scams on social networking sites:

Downloading malware

Many online community sites allow users to upload content to their pages. This often includes music, video, photos, games and other simple programs.

This opens the door to the tricksters who are churning out spyware, trojans and viruses that members then unknowingly either download to their own computers or post on their profile page.

Experts believe this is by far the most common social networking scam.

In a recent attack that hit all the big online communities, a supposed link to a video prompted users to install a plug-in; this then not only installed malware on the victims' PC computers but also mailed itself to everyone on each victim's "friends" list.

According to one expert, the reason social networking sites are particularly vulnerable is because the very essence of an online community is trust. People don't expect to be scammed by other users. That makes them easy prey.

Keeping your Internet security software up to date creates the first line of defense against this sort of attack. You should also be wary about downloading and using new applications from unknown providers.

And just like with email, don't believe that a message you got from a supposed friend or contact necessarily did come from that person.

False identity

It's easy to set up a profile on the big social networking sites. For criminal types, this means an opportunity to pass themselves off as someone else – real or non-existent.

Their motives may just be to have some anonymous fun but they're more likely to be sinister, like establishing phony friendships that lead to face-to-face meetings with who-knows-what consequences, or to float invitations to adult sites.

Sometimes, the scammers use the identities of genuine people, using information and photographs trawled from the Internet. A recent test with a phony user name and page garnered 50 friends in less than 24 hours.

The bottom line: Realize how easy it is to establish phony identities and don't blindly trust that someone is who they say they are. Be wary about accepting new friends you haven't checked out. It's often hard to avoid personal details and pictures of yourself appearing on the Internet, but at the very least, monitor what is available and try to remove anything that could make you vulnerable.

And if you're not a member of these online communities, it's still worth visiting them. Consider setting up a limited user account, or at the very least do a search on your name, just in case someone's pretending to be you.

Identity theft

In addition to passing themselves off as someone else, scammers also steal identities via social networking sites. For a start, individual profile pages often bristle with personal information that can be used for ID theft, such

Continued on Page 6

Voter registration latest target of scammers

The deadline to register to vote for the upcoming election was Saturday, October 4, 2008. **Anyone claiming you can register after this date and be eligible to vote in the upcoming presidential election may be trying to defraud you.**

The South Carolina Department of Consumer Affairs (SCDCA) urges all eligible South Carolinians to vote, but warns there are a number of possible scams concerning the registration of voters.

Scammers are always looking for sensitive information and voter registration is an excellent cover for their sinister operation. Consumers may receive e-mails that offer simple online registration or ask for registration confirmation or corrections. Some consumers may even receive a phone call from someone claiming to be from the election commission or a similar government agency. *These are scams*.

After providing sensitive information, consumers unknowingly release a malicious virus onto their computer. Not only is their personal information now public knowledge, but the scammer now has access to the consumers' financial accounts, online transactions, and identity! Finally, the consumer may think they have registered to vote only to show up at the polls and realize their vote will not count.

Legitimate voter registration forms will NEVER require you to provide financial information of any kind. South Carolina residents will be required to provide their social security number and proof of residency in order to register. Citizens who wish to register to vote should register in person at their county board of voter registration; or they may download a form, complete it, and mail it to their county board of voter registration.

All registration forms must be completed and sent via mail or delivered in person. Consumers should personally deliver or mail their registration forms. Do NOT rely on a third party to handle this important step for you. Consumers who receive e-mails or phone calls from persons claiming to be from the election commission should immediately delete the e-mail or hang up the phone!

Consumers can protect their information by choosing to register on their own and not responding to suspicious offers. For more details on how to register, or to download the proper registration form, consumers can visit the South Carolina State Election Commission at www.scvotes.org.

And another thing...

No matter what anyone tells you, the deadline for voting in this year's presidential race is Tuesday, November 4.

It's not us, it's them!

FDIC warns against spoofed e-mail

The Federal Deposit Insurance Corporation (FDIC) is aware of e-mails appearing to be sent from the FDIC that ask recipients to open and review an attached file.

Currently, the subject line of the e-mail states: "Funds wired into your account are stolen." The e-mail is fraudulent and was not sent by the FDIC.

The fraudulent e-mail tells the recipient that proceeds from identity theft crimes have been wire-transferred into their bank account. The e-mail then directs the recipient to open and review an attached copy of their bank account statement and to contact their bank account managers.

The attached file is actually an executable file containing malicious code or software. Recipients should consider the attached file as a malicious attempt to collect online banking credentials or other personal and confidential information that could be used to gain unauthorized access to online banking services or perpetrate identity theft and other criminal activities.

Recipients of the fraudulent e-mail should not reply and should not attempt to open the attached file.

According to reports received by the FDIC, many antivirus software programs have been detecting and removing the malicious attachment before the e-mail is delivered.

However, if a recipient does open the attachment, the FDIC recommends updating anti-virus software patches and performing a complete scan of the computer and network, if applicable. If a computer becomes infected and the user encounters difficulties removing the malicious code, users should contact their anti-virus software vendor. The FDIC highly recommends using anti-virus software.

For additional information about safe online banking and avoiding online scams, visit www.fdic.gov/consumers/consumer/guard/.

CONTINUED: Lap-locked! How to protect your laptop...

the news or from friends and colleagues. No one thinks their laptop will be stolen — at least not until they find the trunk of their car broken into, notice that their laptop isn't waiting at the other side of airport security, or get a refill at the local java joint only to turn around and find their laptop gone.

Keep in mind the following tips in mind when you take your laptop out and about:

Treat your laptop like cash. If you had a wad of money sitting out in a public place, would you turn your back on it — even for just a minute? Of course not. Keep a careful eye on your laptop just as you would a pile of cash.

Keep it locked. Whether you're using your laptop in the office, a hotel, or some other public place, a security device can make it more difficult for someone to steal it. Use a laptop security cable: attach it to something immovable or to a heavy piece of furniture that's difficult to move — say, a table or a desk.

Keep it off the floor. No matter where you are in public avoid putting your laptop on the floor. If you must put it down, place it between your feet or at least up against your leg, so that you're aware of it.

Keep your passwords elsewhere. Remembering strong passwords or access numbers can be difficult. However, leaving either in a laptop carrying case or on your laptop is like leaving the keys in your car. There's no reason to make it easy for a thief to get to your personal or corporate information.

Mind the bag. When you take your laptop on the road, carrying it in a computer case may advertise what's inside. Consider using a suitcase, a padded briefcase or a backpack instead.

Get it out of the car. Don't leave your laptop in the car — not on the seat, not in the trunk. Parked cars are a favorite target of laptop thieves.

Don't leave it "for just a minute." Don't leave your laptop unguarded — even for a minute. Take it with you if you can, or at least use a cable to secure it to something heavy.

Pay attention in airports. Keep your eye on your laptop as you go through security. Hold onto it until the person in front of you has gone through the metal detector — and keep an eye out when it emerges on the other side of the screener. The confusion and shuffle of security checkpoints can be fertile ground for theft.

Be vigilant in hotels. If you stay in hotels, a security cable may not be enough. Try not to leave your laptop out in your room. Rather, use the safe in your room if there is one. If you're using a security cable to lock down your laptop, consider hanging the "do not disturb" sign on your door.

Use bells and whistles. Depending on your security needs, an alarm can be a useful tool. Some laptop alarms sound when there's unexpected motion, or when the computer moves outside a specified range around you. Or consider a kind of "lo-jack" for your laptop: a program that reports the location of your stolen laptop once it's connected to the Internet.

CONTINUED: E-mail phishing scam asks you to...

original message has been spoofed and the link is phony.

The scam begins with an e-mail containing links to "new" videos on YouTube that are described as "must-see." Users clicking on the link are taken to a fake website closely resembling *YouTube*. The imitation is so good most users were not able to discern that it was a fake.

Users then get a message saying they must download an update to view the latest video. If users choose to go ahead with the download, they are unwittingly downloading malicious programming onto their computer.

The malware is programmed to snoop on online computers, record keystrokes, and recover online passwords or any other confidential information stored offline by users. The victims are usually unaware of what has happened, as the message begins playing a video from the real YouTube site.

SCDCA officials encourage internet consumers to avoid clicking on links forwarded in emails – even if they look legitimate.

"If you want to see what's on YouTube, go directly to YouTube," said Brandolyn Thomas Pinkston, SCDCA Administrator.

"A simple search will take you to the video you want to see." Consumers who want to view SCDCA videos may go to YouTube and type in SC Department of Consumer Affairs, or visit the Department's website: www.scconsumer.gov for SCDCA TV and lots of other helpful information.

Fraud Task Force Contact Information

Consumer Affairs
3600 Forest Drive
Suite 300
P.O. Box 5757
Columbia, SC 29250
www.scconsumer.gov
1.800.922.1594
(803)734.4200

Attorney General's Office
1000 Assembly Street
Suite 519
P.O. Box 11549
Columbia, SC 29211
www.scattorneygeneral.org
(803)734.3970

S.C. Law Enforcement
4400 Broad River Road
P.O.Box 21398
Columbia, SC 29221
www.sled.state.sc.us
(803)737.9000

S.C. Sheriffs' Association
112 West Park Blvd.
P.O.Box 21428
Columbia, SC 29210
www.sheriffsc.com
(803)772.1101

FBI
151 Westpark Blvd.
Columbia, SC 29210
www.fbi.gov
(803)551.4200

U.S. Attorney's Office
1441 Main Street
Suite 500
Columbia, SC 29201
www.usdoj.gov/usao/sc/
(803)929.3000

United States Secret Service
107 Westpark Blvd.
Suite 301
Columbia, SC 29210
www.secretservice.gov
(803)772.4015

S.C. Police Chiefs' Association
4701 Arcadia Road
P.O.Box61170
Columbia, SC 29260
www.scpca.org

CONTINUED: 5 Scams to look out for...

as your age/birth date, your location, phone number, email address, maybe your job and family details and, of course, your photo.

They might try to build on that by phishing for your log-in password. They know that the chances are you use the same password for other sign-ons.

The most common technique is the message through the network that appears to have come from an online buddy, inviting you to check out a new profile page.

Clicking the link takes you to a bogus page that asks you to log on "again." In reality, you're handing over your confidential password to a scammer.

You can limit the risk of this type of identity theft by not posting too much giveaway detail about yourself on your profile page and watching out for suspicious invitations to view another profile.

Beware of any links that ask you to sign on again. This would be very unusual, if not unheard of, if you're already signed on to the network. If the invitation comes via email, contact the friend to confirm he/she sent it.

Profile page hacks

When it comes to social networking scams, it's just as easy for criminals to hack your profile page as it is for them to create their own phony profiles. All they need is your username and password.

Sometimes, hackers do this just for their own idea of having fun, scrawling graffiti over a user's page. Other times they install invisible code that can be used for malicious purposes. Or they simply use your ID as a platform for spamming.

The key to preventing this type of attack is not only to have a strong password but also to change it very frequently.

If your profile or your identity are in any way compromised, you should also inform the site operator. If threats are involved, tell the police.

Sending and receiving spam

Scammers not only want to use your profile to spam others. They want to spam you. And they want to do this with very carefully targeted emails.

Especially on sites for business professionals, they scour members' personal details. They use the sites' own search tools to identify members' areas of expertise and interest. Alternatively, the names and details gleaned are combined together into master lists of people with specific interests that are sold on to other spammers.

Reduce this danger by limiting the amount of information you post on your profile page and listing a short-term or disposable email address for contact.

CONTINUED: Rip-off! Company pressures, threatens businesses to pay for OSHA posters

Do not pay for these.

of Labor or the South Carolina Department of Labor, Licensing and Regulation.

Companies should check with these entities to be sure they have all required materials posted.

Businesses searching the Internet for work posters are advised to be very careful when selecting a website.

Felonious companies often mimic and spoof government websites in an effort to fool businesses into purchasing these free materials.

Real government websites will always have a web address that ends with a .gov extension.