LEVIN, SILVEY, ZELKO & CO., P.A.

Certified Public Accountants

MITCHELL H. SILVEY, CPA
ROBERT A. ZELKO, CPA
BONNIE L. MACKEY, CPA, CSEP

2699 STIRLING ROAD, SUITE B-205
HOLLYWOOD, FLORIDA 33312-6543
(954) 985-8808 (BROWARD)
(954) 985-8839 (FAX)
WWW.LSZCPA.COM

Online Security

You once thought the "boogey man" was scary, but in today's technological world, we're more scared by viruses, hackers and spyware. We need to know how to limit our personal data online, in order to avoid attacks through our internet connections and wireless devices. Another great concern is protecting our children from internet predators.

Nowadays, it's very easy to obtain names, addresses, phone numbers, email addresses, etc. online through a number of search engines. From class reunion sites to internet phone books, we must be "choosy" from the start the amount of personal information supplied and what sites that information is going to. NEVER give out your information to unsolicited email or telephone requests; you should ALWAYS be the initiator of the information divulged. You should conduct an online search to find out where your information (personal and business) is listed. If it's on an unwanted site, request them to remove it, by using the "contact us" link or other remove feature listed.

Shopping online could pose problems if you are not familiar with the vendor and/or their privacy policies. Try to use vendors with secure sites (you'll see the yellow lock or https) and check their buyer/seller feedback before making purchases. You should always read their privacy policy before divulging your personal information and ask questions if uncertain about their information sharing policies. Setting up a separate email for online shopping and newsgroups might prove to be very beneficial. If you have to delete it, you will not disrupt your business email account and should reduce the amount of "spam" you receive on your business account.

Anyone can be a victim of identity theft, online and offline; therefore, learn to protect your personal information. If credit card information, social security numbers, etc. get into the wrong hands, your personal assets (ie. bank accounts), credit record and credit cards are at risk for theft. If you suspect your information has been stolen, visit www.consumer.gov/idtheft to learn what to do. For offline protection, you should make a copy of the contents of your wallet. Make sure to copy both sides of all credit cards, licenses, etc. This will enable you to have all pertinent information if needed to report lost or stolen cards. Keep this copy in a safe place, along with a copy of your passport as well. NEVER preprint your social security number or driver's license number on your checks. You might even consider using your work phone and address or a PO box on your checks instead of your home address. If your credit cards are stolen, you should notify the three national credit report organizations immediately to place a fraud alert on your name and social security number, in addition to notifying the credit card companies. The phone numbers are:

Equifax: 1-800-525-6285
Experian/TRW: 1-888-397-3742
Trans Union: 1-800-680-7289
Social Security fraud line: 1-800-269-0271

You are also entitled to receive an annual credit report online, which should be checked annually to ensure that no fraudulent activity appears. The secure site to obtain your credit report is https://www.annualcreditreport.com.

To help keep your computer safe and secure, use anti-virus software, a firewall and spyware software. As "painful" as all this sounds, they are "necessary evils" in our technological world today! These are like preventative medicine and/or treatments. Most email programs have email filters; however, you should NEVER open any email or download attachments from unknown sources. Also, keep in mind that having the "preview pane" open is the same as opening the mail; therefore, it's too late to avoid a virus coming in. You should close this pane in the email options and be prompted to open any email. If it is uncommon for you to receive attachments from a known source and suddenly you do, DO NOT OPEN the email until you've confirmed with the source that it is a safe and legitimate attachment!

Anti-virus software protects your computer and data from self-replicating programming code that can infect other programs and files. Firewalls protect your computer from hackers, who are individuals attempting to break into your computer to gain access to your personal information. Spyware can be loaded onto your system without your knowledge to monitor your activities and gather your personal information; therefore, anti-spyware software should be installed for added protection. Using strong passwords can prove to be an effective tool in order to protect your information. When setting up passwords, keep the following in mind: have at least 8 characters, including letters and numbers, avoid common words, use different passwords for each online account, and change passwords regularly. If possible, use a combination of a password and PIN.

Bluetooth technology has enabled wireless attacks. Even though Bluetooth has enabled the ease of transferring information and documents, we need to take the necessary steps to protect that information in our cell phones and PDAs. Your Bluetooth device should be set to "undiscoverable" when not in use transmitting data back and forth. "Cybercriminals" actually drive around to detect signals enabling them to "pair" up and hack in to steal your information. These signals can be detected up to one-half mile away! Just as described above for computers, a virus could be installed on your Bluetooth device and wreak havoc with your information in the same manner. A hacker of a Bluetooth phone could make phone calls, send text messages, connect to the internet, etc. Be sure to use strong PIN codes, avoid storing sensitive data, and stay up-to-date on Bluetooth developments and security issues. As with your virus protection updates, it's important to install current security patches on both your Bluetooth devices and computers.

Protecting our children is a major concern not only offline, but online. We've always been concerned about our children walking home or being stalked at the mall, etc.; however, today we must also be concerned about internet predators. Besides the old saying, "never talk to strangers," we must teach our children to "never give out personal information" in chat rooms or bulletin boards online. We've all heard the horror stories on the news about internet predators preying on our young and luring them to another location, only to be taken advantage of! We need to know who our children's online friends are and what sites they are visiting, in order to protect them. The need to discuss and set guidelines and rules for computer/internet use and possibly keeping the computer in a central area are becoming more and more necessary. You can also implement parental controls and firewall locks (just like in your office) to block unwanted pop ups and/or illegal sites. Other considerations may be installing software to monitor web traffic and partitioning your computer into separate operating systems (protecting your partitioned information). If you believe your child is in danger, you can visit www.getnetwise.org and/or http://staysafeonline.info for additional information.

There are numerous sites and vendors that have software and hardware for varying degrees of online security and information. If you suspect that you've been "hacked," "spammed," or received a virus, you should immediately unplug the phone/cable line from your computer and scan your computer with updated anti-virus software and update your firewall. You can also report your problem to the FBI at www.ifccfbi.gov. If internet fraud is suspected, you can report it to the FTC at www.ftc.gov and for deceptive spam forward the email to spam@uce.gov. For more information, please contact: Bonnie Mackey

November 2005