E-SAFE TECHNOLOGIES

The E-Insider

"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

Broken Hearts and Stolen Data

While many people buy their significant other a box of decadent chocolates, a dozen red roses or an oversize teddy bear for Valentine's Day, there are a few people who are going to go home with a broken heart as their personal information is stolen right from under them. It's a harsh reality, but both individuals and businesses are constantly targeted by fraudsters and hackers who want to steal any bit of data that will make them money.

You may have taken all the precautions to protect yourself and your business – but what do you do if it does happen? Just as when a lover breaks your heart, you have to move on, get back on your feet and work your way through this unfortunate circumstance.

Once your data is stolen, it's gone. Credit cards can be canceled, but other information, such as your name, address, social security number and more, can be more difficult to control.

In 2014, social media accounts, such as Twitter, became more valuable to hackers than credit cards. These types of accounts are hot commodities on black markets.

Does that mean you should be worried with all the information you have stored online? Absolutely not!

If you do fall victim to a data breach, you can still protect yourself!

Contact your credit card companies. Let them know you suspect your credit card info has been compromised. They will work with you to ensure you don't face financial losses.

Keep a close eye on all your accounts. Watch for suspicious activity and report it when you see it.

Change your passwords. This is particularly critical if you used a single password for multiple services.

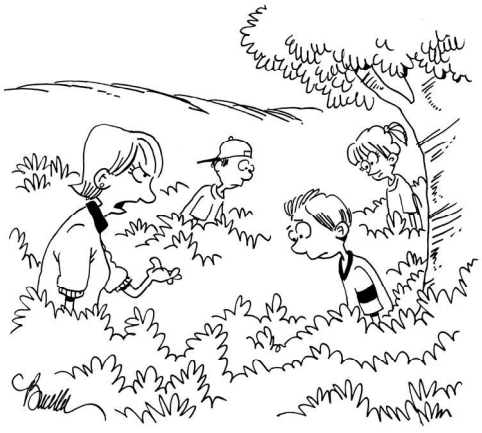
Use a credit-monitoring service. They aren't designed to prevent data from being stolen, but in the event of a breach, you'll be notified immediately so you can take action.

Give us a call at 412-944-2424 and we'll put together a plan to keep your company's data secure.

"As a business owner, you don't have time to waste on technical and operational issues. That's where we shine! Call us and put an end to your IT problems finally and forever!"
- Tim Steinour,
E-Safe Technologies

February 2015
Pittsburgh, PA

Inside This Issue…



"Sure, it's all fun and games until someone loses an iPhone."

How To Keep Your Laptop Secure When Using Public WiFi Hotspots

They are everywhere these days. WiFi hotspots for checking e-mail and hopping on the Internet can be found in airports, coffee shops and even most fast-food joints. But have you ever wondered, just how safe is it to connect? With the proliferation of hackers, viruses and identity theft at an all-time high, you are smart to be concerned. Unfortunately, it is easy for a hacker to set up a WiFi spot to access your laptop, called an "evil twin." An evil twin is a wireless hotspot that is used to lure people from a nearby, legitimate hotspot. For example, when logging in at your favorite coffee shop, you may have inadvertently logged in to an evil twin Internet connection set up by the person working on a laptop at the next table.

Just like legitimate sites, evil twins allow you access to the Internet, but in the background they record everything you are typing. Log on to your e-mail, investment web site or bank account, or buy something online, and they are recording your keystrokes.

Tip: Do you want an easy way to securely access your network and the Internet from anywhere? Call us today at 412-944-2424 about setting up a VPN for your office!

You may be asking, "How do I protect myself at WiFi hotspots?" First you need to make sure the hotspot is legitimate. You can do this by asking someone who works at the WiFi location; in fact, some businesses will give you printed instructions that include the hotspot name. Even here you need to be careful. Many times, in an attempt to make you feel comfortable, the hacker will use an evil twin name that mimics the legitimate hotspot and, on some occasions, the fake site may even show up at the top of your network list by having a stronger signal than the legitimate site.

The best protection you can have is connecting via your company's VPN (virtual private network).

A VPN protects your online information by encrypting your data and activity even if you're connected through an evil twin. If you don't have a VPN, the best protection is to surf the net, but never type in password, credit card, social security, bank account or other sensitive information when connected to a public WiFi hotspot.

E-SAFE Technologies 6th Annual Customer Appreciation Event!!!

Start Date & Time: March 19th, 2015 8:15 AM Registration Begins
End Date & Time: March 19th, 2015 3:30 PM

Guest Speaker: Former Pittsburgh Steeler Craig Wolfley
Listen to Craig Wolfley's dynamic talk on his life through light, humorous and inspiring tales about his 12 years as a player in the NFL and his life after football.

Come to our event to hear:

- Come learn about the latest product and solutions from industry leading technology vendors such as **Nimble Storage**, **Veeam**, **VMware**, **Cisco**, **Solutionary** and **BlackBox.**
- Hear about the latest threats in ***Data Security*** and ***Global Threat Intelligence***.
- Understand the benefits of Managed IT Services and how this model can ***save your business*** *$$$*.
- Discuss the latest in ***Virtualization Monitoring*** and how new tools can make your job easier!

New Venue: Latitude 360 in Robinson

200 Quinn Drive Pittsburgh, PA 15275 | 412-693-5555

Register today!!! www.e-safetech.com/marchmadness

Shiny New Gadget Of The Month:

Prizm

This month's gadget is so new, it isn't even off the assembly line. Meet Prizm — a small, pyramid-shaped device designed to make your home-audio experience as hands-off as humanly possible. The device was recently backed on Kickstarter this past November. The French company behind the audio device wanted to create an intuitive music experience that brings users new music, while learning what they really love to listen to.

The device streams music from cloud services such as Deezer, Spotify and SoundCloud, with more services planned in the future. It works by accessing your WiFi network. It doesn't contain any speakers, so you'll have to supply your own (it connects via Bluetooth, 3.5 mm stereo jack and optical audio). And despite being called hands-off, the device sports buttons to let you like or skip songs to customize your listening experience.

It can currently be pre-ordered from www.meetprizm.com for $139.

HOW TO GROW STAR PERFORMERS

A study of computer programmers at Bell Laboratories showed that the star performers outperformed moderate performers by a margin of 8 to 1. If that holds true in your organization, the conversion of five of your moderate performers into star performers would be the equivalent of adding 35 moderate performers to your workforce. Where are you going to find the five additional star performers? You don't find them. You develop them.

The Bell Labs study identified nine work strategies that characterize star performers. All of them are qualities that can be inculcated through a good corporate education system. According to researchers Robert Kelly and Janet Caplan, these qualities are:

1) **Taking initiative:** accepting responsibility above and beyond your stated job, volunteering for additional activities and promoting new ideas.
2) **Networking:** getting direct and immediate access to coworkers with technical expertise and sharing your own knowledge with those who need it.
3) **Self-management:** regulating your own work commitments, time, performance level and career growth.
4) **Teamwork effectiveness:** assuming joint responsibility for work activities, coordinating efforts and accomplishing shared goals with workers.
5) **Leadership:** formulating, stating and building consensus on common goals and working to accomplish them.
6) **Followership:** helping the leader to accomplish the organization's goals and thinking for yourself rather than relying solely on managerial direction.
7) **Perspective:** seeing your job in its larger context and taking on other viewpoints, like those of the customer, manager and work team.
8) **Show-and-tell:** presenting your ideas persuasively in written or oral form.
9) **Organizational savvy:** navigating the competing interests in an organization, be they individual or group, to promote cooperation, address conflicts and get things done.

Star performers considered initiative, technical competence and other cognitive abilities to be core competencies. Show-and-tell and organizational savvy were on the outer edge of their circle of importance. Middle performers placed show-and-tell and organizational savvy at the center. While star performers were focused on performance, middle performers were focused on impressing management.

Star performers and middle performers also showed marked differences in their attitudes toward networking. The middle performers waited until after they had encountered problems before looking around for someone who could provide help and support. The star performers built a network of helpers and supporters in advance, so they could call on them immediately when needed.

The study concluded that "Individual productivity… depends on the ability to channel one's expertise, creativity and insight into working with other professionals."

Star performers emerge from educational systems tailored to the individual company and the individual job. They don't want to become clones. Too many companies today are content with training programs that provide people with knowledge and expertise, but skimp on educational processes that teach them to apply what they learn. You can't train them to seek excellence. You change that attitude through consistent input that appeals to an individual's self-interest and organizational spirit.

Protect Yourself From Online Credit Card Fraud

The past couple of years have been a rough ride for anyone who relies on a credit card to make purchases. Data breaches have plagued retail stores in the U.S. and Canada. Credit card providers are set to roll out new, more secure credit cards to consumers this year, catching up to Europe and much of Asia in terms of credit card security. The U.S., in particular, has lagged behind in credit card security due in part to the cost of upgrading both the cards themselves and the pay terminals.

If you are concerned about your credit card information falling into the wrong hands, there are several steps you can take to protect yourself:

Only give your credit card information to secure and trusted web sites. Never enter any personal or financial information on a non-secure web page. If you don't see "https" in the web address, move along.

Monitor all activity. Regularly check your credit card and bank statements. The simplest way to spot fraud is to monitor all your financial activity. Many credit card providers have custom alerts you can set to notify you if certain purchases are made.

Never save credit card information. Many online retailers and shops now ask if you would like to save your credit card information for future use. While it may seem convenient, skip it.

Delete your cookies and auto-fill data. When you enter information on a web page, that data is stored in your web browser. After you complete a transaction, go into your browser's options, settings or history tab and delete the data.

Employee of the Month:

E-Safe is pleased to highlight Aireal McCullough as our February 2015 Employee of the Month! Aireal has already made a significant impact at E-Safe and we are thrilled to have Aireal as part of the E-Safe team!

A native of Pittsburgh, Aireal loves to cheer on the Pens when she's not spending her time reading, hiking, kayaking, camping or volunteering. In fact, if Aireal didn't find her way into the wonderful world of IT, she considered working with an International mission group in Rwanda. This would have been a perfect fit since Aireal has already spent much of her time in Mexico helping others in need.

Luckily for E-Safe, Aireal decided to take a role within the organization as a Solutions Engineer since she has a strong background in working with Cisco networking solutions and holds many specializations and certifications such as a CompTia A+ certification. As a graduate from the Parkway West Career and Technology Center for Information Technology, Aireal is the perfect fit as a Solutions Engineer.

WELCOME ABOARD AIREAL!!!

The Lighter Side:

Punch a Painting, Go to Jail

In 2012, Andrew Shannon punched a Monet painting valued at $10 million. The incident occurred at the National Gallery of Ireland, located in Dublin. The painting, entitled *Argenteuil Basin with a Single Sailboat*, painted in 1874, apparently represented something much greater to the man who decided to attack it.

Right after his initial arrest, Shannon said the attack represented his way of "getting back at the state." Later on, when he appeared in court, he changed his tune. Instead of an "attack against the state," he said the whole thing was just a big misunderstanding. He said he didn't punch the painting, he "fell into it." He told the court he had felt faint and fell. The painting just happened to be in his way.

Fortunately, the National Gallery has plenty of CCTV cameras and the whole thing was recorded. What did those cameras see? Andrew Shannon very deliberately thrusting his fist through the Monet painting. In December of 2014, he was sentenced to five years in prison, and *Argenteuil Basin with a Single Sailboat* is back on display after being fully restored.

G