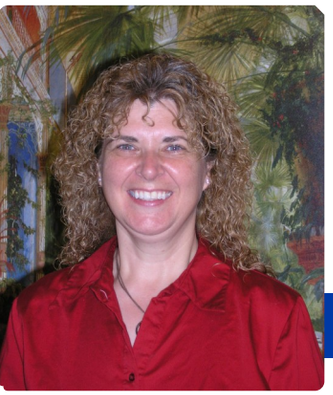

szymanski
CONSULTING

June 2013

Cathy's Message

WOW! Time is certainly flying by. I am shocked that June is upon us.

I for one am not even close to being ready for the summer. I am still getting ready for Christmas 2012. Guess it makes me this much closer to being ready for this year.

I hope you have taken time to read about our security conference. We still have seats available and would love to have you join us.

With the news on companies like Apple, Google, EMC and The New York Times being hacked, we all need to be more concerned about security. We are all vulnerable to hacker attacks, possibly even more so. You never know who may stumble across a crack in your network's firewall and breach your network security. Cyber Security is a big threat, and that is why we are offering this conference to you, so that you can educate yourself and your staff.

This is going to be an amazing event filled with information for you to take back to the office. This is not a sales event , but more of a educational event.

If you have questions please let me know.

This past month has certainly been a busy month for Szymanski Consulting, we are very pleased to welcome a new person to our team. You will hear more about him next month. His name is Scott McHenry. We have been keeping Scott very busy, and many of you have had the privilege of working with him already.

If there is anything you would like us to sell, please let us know. We are here for you, whatever we can do to make your job easier and reduce your TCO. Thank you for

Videos

We hope you are enjoying our weekly videos. If you have a specific topic you would like to see us cover please let us know.

If you would like us to add someone onto the list we will certainly take care of that.

We feel the more education we can get

Security Awareness Conference

Szymanski Consulting, Inc., and the Better Business Bureau have teamed up to bring a security awareness event to the Bayfront Convention Center on June 6, 2013.

Topics:

Data Breach and Cyber Liability, presented by
Will Collins, Northwest Insurance Services

Social Media Security, presented by
Lesley Ridge, Socialution Media, LLC

Banking Security, presented by
Allan Krayeski and
Renee Santos, First National Bank

On-Line Security, presented by
Corporal Stewart, PA State Police

Secure Your ID, presented by
Warren King Better Business Bureau

Disaster Recovery, presented by
Cathy Szymanski, Szymanski Consulting

Security Issues in Document Retention, presented by
Robert C. LeSuer, Elderkin Law Firm

Please Make sure you RSVP your seat.
Lunch is included.
Register at www.szy.com/event
use **PROMO CODE: SZY2**

Registration will be at 9:30 a.m. with the event beginning at 10:00 a.m. The event will end by 2:30 p.m.

Who should attend?

- Business Owners, managers and Executives interested in the security of their business.

Why should you attend?

- Stay current on cyber security threats, vulnerabilities and exploits
- Cost effective security training and peer networking
- Find help for information security issues

Conference Goals:

- Educate the community
- Increase awareness about cyber security threats and risks
- Sharpen technical skills
- To ensure participants leave the event with practical information that can be applied directly to their specific cyber security environment

If you have any questions, please contact Cathy@szy.com or call her at 814-455-6069 x300

Feel free to pass this on to colleagues.

7 Reasons Why It's Time To Give Up On Windows XP, Once And For All

Although businesses have been getting rid of Windows XP for at least the last 3 years, the fact remains that as of last December, around 500 million users will still be running Windows XP. Here are 7 of the top reasons it's time to finally give up Windows XP now.

1. **Tons Of Viruses.** There is a huge library of viruses aimed at Windows XP and limited antivirus support still available.
2. **XP Is OLD (almost 12 years old!).** The 1st iPod was released the same year as Windows XP. In a world where the 5th iPhone has been released, no one should be left using an O/S that pre-dates the 1st *iPod!*
3. **Least Secure Operating System (By Far!).** ALL other platforms, including Linux, all versions of Mac OS X, Windows 7 and Windows 8 are more secure than XP by a huge margin. Windows Vista is actually a far safer option (scary!).
4. **Built For A Simpler Time.** XP was created for a simpler world of technology. It was formatted to fit to a screen only 640 pixels wide, and it showcased IE6 as a new product. The internet was a different place when XP was developed. Smartphones were non-existent, laptops were a luxury and tablet computers were science fiction.
5. **No More Band-Aids.** Only so many band-aid fixes on top of each other can be effective.
6. **Support Is Ending.** Mainstream support of XP ended 4 years ago (April 2009) with only critical security updates since then.
7. **Malware Everywhere.** You can continue to use XP, but with more malware than ever. XP is by far the most vulnerable platform to connect to the internet.

Microsoft Word Shortcut Keys

We hope you are enjoying our monthly shortcut tips. If there are tips you would like to share with everyone, please send them to us and we will post them in our monthly newsletter.

The following tips are for Outlook 2010

Ctrl +N	Create a new document
Ctrl +O	Open a document
Ctrl + W	Close a document
ALT+CTRL+S	Split the document Window
Ctrl +S	Save a document
Ctrl +B	Make letters bold
Ctrl + [	Decrease font size 1 point
Ctrl + [	Increase font size 1 point

Are You Getting "Scroogled" By Google?

If you use Google for search, Gmail for e-mail or an Android phone as our smart phone then, according to Microsoft, you're getting "scroogled" daily! What exactly does that mean? Well according to www.scroogled.com it means that Google systematically uses your private information that it collects online through your search, your emails, your Android app store purchases and more to sell more ads.

And there's no way to opt out.

Let me explain further how they do this with a few examples

- **Gmail**: Google's systems go through all of your personal Gmail emails ever sent and received looking for keywords they can use to target you with paid ads. So that email you just sent to your spouse, your child or whomever you sent it to...Google is looking to see how they can use that to target you with advertisements. 46% of users of the e-mail service don't' even know it. Great for advertisers. Not so great for your privacy.
- **Google Android App Store:** When you buy an Android app from the Google App Store, they give your full name, e-mail address and the neighborhood where you live to the app maker. This occurs without clear warning to you every time that you buy an app. That might be OK in a handful of instances, but it's impossible to tell what the app maker might do with that information. App makers are spread all around the world and not all app makers are trustworthy.

Consumer Privacy Groups are up in arms about this blatant sharing of your personal information. A Consumer Watchdog Complaint to the Federal Trade Commission on Feb. 25, 2013 said "The various applicable Google privacy policies promise not to share user information collected by Google outside of the company. The policies contain no exceptions that would justify Google's disclosure to app developers of confidential user information."

In full disclosure, the term "Scroogled" has recently been hyped up in a series of big marketing campaigns bashing Googles' services. So are these privacy concerns a bunch of marketing hype or real concerns to act on? That answer is really up to you.

What to do now? Only you can determine how much you want to risk your own personal information in the hands of Google. The online world has an increasing number of security risks to consider these days and most of them don't' have anything to do with Google. How do you respond? Hopefully by being informed and making decisions basked on real information and not because you didn't know any better.

All About Trusted Contacts

The increasing popularity of social media has brought with it an increase in the number of security issues. Facebook, the most popular platform, has integrated fairly robust security measures to keep your account secure. A recently introduced new security feature-Trusted Contacts-uses your friends to help you regain access to your account.

Trusted Contacts was officially introduced by Facebook in early May 2013, after nearly two years in testing. It is a potentially really useful feature that could help you out one day.

What exactly is Trusted Contacts?

According to Facebook, "Trusted Contacts lets your friends help you if you're having trouble logging into your account. "if you have been previously using the Trusted Friends feature, this has now been renamed and merged with Trusted Contacts.

Trusted Contacts allows users to set up to five Facebook friends who can help you regain access to your account. For example, if you forget your password your nominated friends can send you a phrase to enter so that you can get back into your account.

It is a good idea to set this up, but beware that at least three friends who set as a Trusted Contact will need to send you a private code before you can regain access. The friends will only have access to the code if they log into Facebook, so make sure you pick someone who is able to log into Facebook regularly.

How to set up Trusted Contacts

1. Logging into your Facebook profile and clicking on the cog at the top right-hand side of the window.
2. Selecting Account Settings followed by Security in the window that opens.
3. Clicking on Edit beside the Trusted Contacts field followed by Choose Trusted Contacts.
4. Typing the names of three to five reliable friends. You should see the name of each friend in a blue box below the search bar.
5. Click Confirm.

Facebook will notify the contacts you've selected with more information about how the process works.

If you are having trouble accessing your Facebook account you can tell your trusted friends to visit facebook.com/recover to get the code and then pass it to you. Once you have entered three codes, provided by your friends, you should be able to get into your profile.

Trusted Contacts could be a useful tool, especially if you don't' use or access your personal Facebook profile on a regular basis. It's important to stress that you pick someone you trust,

Taking Referrals

Do you have anyone you would like to refer to us! We have a referral program that we would love to share with you. Please email Cathy today to find out more information.

Five Steps To Protect Your Business From Cyber Crime

A Seattle company was recently broken into and a stash of old laptops was stolen. Just a typical everyday crime by typical everyday thieves. These laptops weren't even being used by anyone in the company. The crime turned out to be anything but ordinary when those same thieves (cyber-criminals) used data from the laptops to obtain information and siphon money out of the company via fraudulent payroll transactions. On top of stealing money, they also managed to steal employee identities.

Another small company was hacked by another "company" that shared the same high-rise office building with them. Management only became aware of the theft once they started seeing unusual financial transactions in their bank accounts. Even then, they didn't know if there was internal embezzlement or external cyber theft. It turned out to be a cyber theft. The thief in this case drove a Mercedes and wore a Rolex watch...and looked like anyone else walking in and out of their building.

You Are their Favorite Target

One of the biggest issues facing businesses in the fight against cybercrime is the lack of a cyber-security plan. While 83% lack a formal plan, over 69% lack even an informal one. Half of small business owners believe that cybercrime will never affect them. In fact, small businesses are a cybercriminal's favorite target! Why? Small businesses are not prepared and they make it easier on criminals.

The Result? Cyber-attacks cost an average of $188,242 each incident and nearly two-thirds of the businesses affected are out of business within six months (2011 Symantec/NCSA Study) A separate study by Verizon showed that over 80% of business cybercrime victims were due to insufficient network security (wireless and password issues ranked highest). With insecure networks and no formal plan to combat them, we make it easy on criminals.

How They Attack

The #1 money generating technique these "bad guys" use is to infect your systems with malware so that whenever you (or your employees) visit a web site and enter a password (Facebook, bank, payroll etc.) the malware programs harvest that data and send it off to the bad guys to do their evil stuff.

They can get to you through physical office break ins, "wardriving" (compromising defenseless wireless networks) or email phishing scams and harmful web sites. Cyber-criminals are relentless in their efforts, and no one is immune to their tricks.

5 Steps To Protect Your Business

1. **Get Educated.** Find out the risks and educate your staff.
2. **Do A Threat Assessment.** Examine your firewall, antivirus protection and anything connected to your network.
3. **Create A Cyber-Security Action Plan.** Your plan should include both education and a "fire-drill."
4. **Monitor Consistently,** Security is never a one-time activity. Monitoring 24x7 is critical.
5. **Re-Assess Regularly.** New threats emerge all the time and are always changing.
6. **Come to our security event on June 6, at the Bayfront Convention Center. See front page for information.**

szymanski CONSULTING

Attend our
'Security Event' on
June 6th
for more information.

Varnex™

Microsoft Partner
Gold Desktop
Silver Midmarket Solution Provider

Kroll Ontrack.

Szymanski Consulting, Inc.
8127 Nathan Circle
Erie, PA 16509
814-455-6069
www.szy.com

szymanski CONSULTING