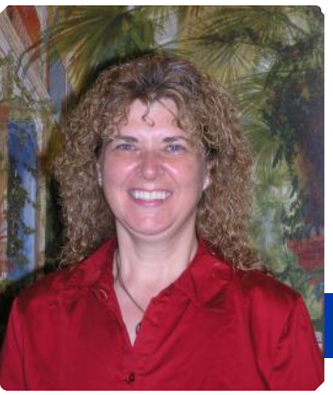


szymanski
CONSULTING

March 2014

Cathy's Message

Even though it is very cold outside, we all know that Spring is right around the corner. I love spring time, it is a time for Spring flowers, warmer weather and I find people are more cheerful in the spring.

We are very excited to announce we that Kevin R. and his lovely wife had a healthy baby boy. Everyone is doing well, and Kevin thanks everyone for their well wishes and concerns.

Hopefully you no longer have any XP machines, however; if you do, please give us a call. XP will no longer be supported after April 9th, 2014.

Are you following us on Facebook? Please like our page at **www.facebook.com/szycom**

We hope you know how much we appreciate each and everyone of you. Take care and have the best day ever.

Cathy & David.

What is Spear Phishing?

Spear phishing is a specialized type of phishing that instead of targeting a mass number of users, as normal phishing attempts, targets specific individuals or groups of individuals with a commonality e.g., an office.

A hacker will first pick a target and then try to learn more about the related people. This could include visiting a website to see what a company does, who they work with, and even the staff. Or they hack into a server in order to get information.

Once they have some information, usually a name, position, address, and even information on subscriptions, the hacker will develop an email that looks similar to one that another organization might send e.g., a bank. These emails are often similar to official correspondence and will always use personal information such as addressing the email to you directly instead of the usual 'dear sir or madam'. The majority of these emails will request some sort of information or talk about an urgent problem.

Continued on page 2...

Are Your Employees "Cyberloafing"

Are you paying 80% of your employees to "Cyberloaf" on the internet, Watching Cat Videos, Searching For a better Job, or Accidentally Downloading a Virus on your network?

Recently, we have seen a dramatic increase in the number of local businesses suffering significant financial and productivity losses due to employees inappropriately using their Internet access during work hours – and much of this is fueled by social media sites such as Facebook and YouTube. Studies have shown that between 60 and 80 percent of people's time on the Internet at work has nothing to do with work!

What makes this situation so dangerous is that the majority of business owners don't even realize that it's going on until it's too late. By then they have found themselves in the middle of a costly and embarrassing lawsuit because an employee posted something inappropriate online OR downloaded a virus.

In other cases, the owner NEVER finds out, but is inadvertently losing THOUSANDS of dollars because employees are spending 2-3 hours a day to goof off online – and you're footing the bill.

And age of the employee doesn't affect an employee's ability to waste time on the Internet. Older employees do things like managing their finances while younger employees check social media.

A Company Internet Policy Is NOT Enough

A recent study showed that the presence of a strong Internet policy at work was not enough to curb activity, as many employees don't think it's wrong to surf the web and a policy was not going to change their minds. Unfortunately, the only way to curb this activity is not only to threaten consequences, but to actually take action and reprimand employees.

If you would like to discuss your Internet and E-mail Usage call our office at 814-455-6069 x 300, email cathy@szy.com.

St. Patrick Day Trivia

I love St. Patrick's Day, seeing so many people wearing something green. I often wonder if they dig through their closets every year to find something green, or do they go out and purchase that green shirt for this one day a year event.

St. Patrick's day was originally a religious holiday to honor St. Patrick, who introduced Christianity to Ireland in the fifth century, St. Patrick's Day has evolved into a celebration for all things Irish. The world's first St. Patrick's Day parade occurred on March 17, 1762 in New York City.

About 24% of the Boston metropolitan area population claims Irish ancestry, one of the highest percentages for the top 50 metro areas by population.

The harp is the symbol of Ireland. The color green is also commonly associated with Ireland, also known as "the Emerald Isle"

The Irish flag is green, white and orange. The green symbolizes the people of the south, and orange, the people of the north. White represents the peace that brings them together as a nation.

The name "leprechaun" has several origins. It could be from the Irish Gaelic word "leprechaun", which means "a kind of aqueous spirit' Or, it could be from "leath bhrogan", which means "shoemaker."

According to the Guinness book of World Records, the highest number of leaves found on a clover is 14. One estimate suggest that there are about 10,000 regular three-leaf clovers for every lucky four-leaf clover. Legend says that each leaf of the clover means something, the first is for hope, the second for faith, the third for love and the fourth for luck.

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.

What is Spear Phishing?

Continued from page 1...

Somewhere in the email will be a link to the sender's website which will look almost exactly like the real thing. The site will usually ask you to input personal information e.g., an account number, name, address, or even passwords. If you went ahead and followed this request then this information would be captured by the hacker.

What happens if you are speared?

From previous attack cases and reports, the majority of spear phishing attacks are finance related, in that the hacker wants to gain access to a bank account or credit card. Other cases include hackers posing as help desk agents looking to gain access to business systems.

Should someone fall for this tactic, they will often see personal information captured and accounts drained or even their whole identity stolen. Some spear phishing attacks aren't after your identity or money, instead clicking on the link in the email will install malicious software onto a user's system.

We are actually seeing spear phishing being used increasingly by hackers as a method to gain access to business systems. In other words, spear phishing has become a great way for people to steal trade secrets or sensitive business data.

How do I avoid phishing?

Like most other types of phishing related emails, spear phishing attempts can be easy to block. Here are five tips on how you can avoid falling victim to them.

Know the basic rule of business communication - The most important one you should be aware of is that the majority of large organizations, like banks, social media platforms, etc., will not send you emails requesting personal information. If you receive an email from say PayPal asking you to click a link to verify your personal information and password, it's fake and you should delete it.

Look carefully at all emails - Many spear phishing emails originate in countries where English is not the main language. There will likely be a spelling mistake or odd wording in the emails, or even the sender's email address. You should look out for this, and if you spot errors then delete the email immediately.

Verify before you click - Some emails do have links in them, you can't avoid this. It is never a good idea to click on these without being sure. If you are unsure, phone the sender and ask. Should the email have a phone number, don't call it. Instead look for a number on a website or previous physical correspondence.

Never give personal information out over email - To many this is just plain common sense – you wouldn't give your personal information out to anyone on the street, so why give it out to anyone online? If the sender requires personal information try calling them or even going into their business to provide it.

Share only essential information - When signing up for new accounts online, there are fields that are required and others that are optional. Only share required information. This limits how much a hacker can get access to, and could actually tip you off. e.g., they send you an email addressed to Betty D, when your last name is Doe.

Keep your eyes out for the latest scams - Pay attention to security websites like those run by the major antivirus providers, or contact us. These sites all have blogs where they post the latest in security threats and more, and keeping up-to-date can go a long way in helping you to spot threats.

If you are looking to learn more about spear phishing or any other type of malware and security threat, get in touch.

Email Etiquette

In today's business world, e-mail is a very useful tool for communication. It is a quick and easy way to relay a message to another, as opposed to leaving a garbled voicemail if the recipient is currently unavailable. Because of the lack of personal interaction involved with e-mail, there are certain guidelines that should be used when writing an e-mail so that it can be as effective as possible.

Keep messages brief and to the point. Concentrate on one subject per message whenever possible. Just because your writing is grammatically correct does not mean that it has to be long. Nothing is more frustrating than wading through an e-mail message that is twice as long as necessary.

Refrain from sending one-liners. "Thanks," and "Oh, OK" do not advance the conversation in any way. Feel free to put "No Reply Necessary" at the top of the e-mail when you don't anticipate a response.

Respond in a timely fashion. Unless you work in some type of emergency capacity, it's not necessary to be available the instant an e-mail arrives. Except in an emergency, if someone does not immediately respond to an email, follow up e-mails and phone calls are not necessary. Depending on the nature of the e-mail and the sender, responding within 24 to 48 hours is acceptable.

Pick up the phone. If a topic has many parameters that may need explained or will generate many questions or confusion, e-mail should not be used. Use the phone as opposed to e-mail based on the situation. If information needs to be distributed to a large group, sending an e-mail is useful. You should use the phone when cancelling events such as meetings, interviews or lunches last minute.

Don't use e-mail as an excuse to avoid personal contact. Don't forget the value of face-to-face or even voice-to-voice communication. E-mail communication isn't appropriate when sending confusing or emotional messages. Think of the times you've heard someone in the office indignantly say, "Well, I sent you e-mail." If you have a problem with someone, speak with that person directly. Don't use e-mail to avoid an uncomfortable situation or to cover up a mistake.

Remember that e-mail isn't private. I've seen people fired for using e-mail inappropriately. E-mail is considered company property and can be retrieved, examined, and used in a court of law. Unless you are using an encryption device (hardware or software), you should assume that e-mail over the Internet is not secure. Never put in an e-mail message anything that you wouldn't put on a postcard. Remember that e-mail can be forwarded, so unintended audiences may see what you've written. You might also inadvertently send something to the wrong party, so always keep the content professional to avoid embarrassment.

If your email is emotionally charged, walk away from the computer and wait to reply. Review the Sender's email again so that you are sure you are not reading anything into the email that simply isn't there.

Set up signatures for mobile devices. The signature should inform the recipient that you are sending from a mobile device such as a phone or a tablet. This lets the recipient be aware of why there are typos, or why your response may seem short.

Do not over use 'High Priority.' Only mark an email as high priority when completely necessary. When recipients receive too many emails marked as high priority from the same sender, it loses its intended purpose.

Formatting. When sending e-mails, don't use patterned backgrounds, as these make it harder to read. When emphasizing a point, use **bold**, *italics*, and <u>underline</u> sparingly. These elements are used to catch the eye letting the recipient know what you are emphasizing. Overuse, much like the above mentioned high priority, takes away from the intended function.

DR Plans Are Vital For Your Business

Small to medium businesses continue to struggle when developing a comprehensive disaster recovery plan. DRPs or Disaster Recovery Plans, can spell the difference between your business's outright destruction when unforeseen calamities occur or a careful and systematic recovery to normal operations with little loss to operations or profits.

When creating a disaster recovery plan for your business, there are certain key elements that you need to consider.

Basics of a Disaster Recovery Plan

In building an effective disaster recovery plan, you should include documentation that lays out the details of the ins and outs of the plan. You need to know that there is no right type of DRP, nor is there a single template that fits all. But there are three basic aspects to a disaster recovery plan: Preventive measures, detective measures, and corrective measures.

In addition, before building your disaster recovery plan, make sure that it can provide an answer to these basic questions:

> What is the objective and the purpose of making one?
>
> Who are the assigned team responsible when certain events occur?
>
> What is the framework and the procedure to be followed?

Plan for the worst case scenario

Since you're planning for an unforeseen event, you might as well make sure that you have plan for the worst case scenario. That way, you'll never be overwhelmed and you're as prepared as you can be for any situation.

Having different tiers of backup plans is also advisable. It gives you a better assurance that when bad comes to worst, you have a system in place to make sure that these disasters are handled correctly, regardless of the disaster's severity.

Data issues

One of the objectives of disaster recovery plan is to protect the collection of data. Almost half of the total population of business organizations experiences data loss from both physical and virtual environments. This is often due to corruption of the file system, broken internal virtual disks, and hardware failures. Thus, there is a real need for established data recovery plans such as backup features offered by many IT solution vendors.

Test-drive

Before deploying your disaster recovery plan, you need to have a test-drive to check if it works. Aside from making it work, you also need to know if it's going to be effective. Through testing, any shortcomings can be identified and will garner corresponding resolutions to improve on your plan. Although the real score of its effectiveness can only be identified once a disaster occurs, at least you will have an idea of how your business and the recovery plan can operate during a disaster.

Building an effective disaster recovery plan is a must for your business. This might not directly lead to a positive impact on productivity but it will surely save you in the events that can possibly crush your business. Anticipating and adjusting for the things that might happen is one of the keys to a company's success.

Setting up an effective DRP can be quite an intricate process since there are several elements that you need to consider. Should you want to learn more, give us a call and we'll have our associates help you develop and test a plan that works best for your business.

Client Spotlight

Szymanski Consulting, Inc. is pleased to welcome **The Vargo Company** as a new client.

The Vargo Company is an independent, full service, third party administration firm of qualified retirement programs located in Erie with over 100 years of combined experience in administering defined contribution plans and employee stock ownership plans.

With over 475 clients ranging from one person sole proprietorships to large corporations competing in the global marketplace, The Vargo Company serves industries from financial, manufacturing, trade, medical and service sectors of the economy.

The hallmark of The Vargo Company is its high level of customer service to their clients. This occurs in several ways such as the expertise in designing a plan to meet each client's individual needs and continuing with supporting a client's day-to-day plan administration.

"Our customer service allows clients to know who they are talking with on a daily basis and to work with clients on the design of retirement programs unique to them," said John Sample, Owner of The Vargo Company. "We are not a cookie cutter shop and our accountability to clients adds critical value to them."

As a small business, The Vargo Company recognizes the vital role of technology to support their clients. "Szymanski's IT expertise with the managed services program ensures our technology from workstations, software, to the server is working at the highest level so we can deliverer on our commitments to clients," said Sample.

For more information on The Vargo Company please visit www.TheVargoCompany.com or call John Sample, Owner at 814-897-1180.

Shiny New Gadget

Nest Protect

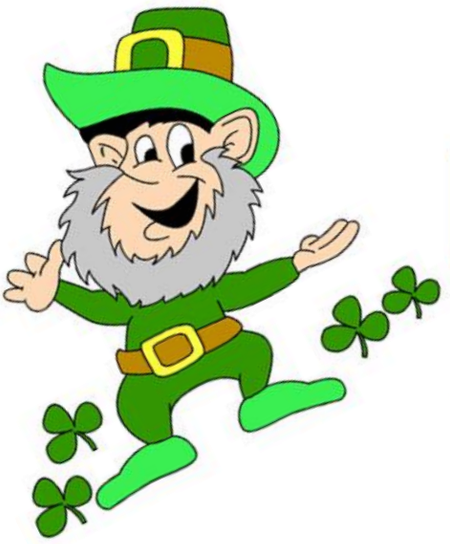
The Nest Protect Motto: Safety shouldn't be annoying.

We have all experience it. That annoying low-battery chirp that 9 times out of 10 wakes you from a dead sleep. Why is it that the smoke alarm battery inevitably runs low in the middle of the night? Then it happens…in your half-awake stupor, you rip it from the wall with intentions of re-hanging it in the morning. More times than not, you forget to replace the batteries and re-hang it and then there you are with no warning system should a fire break out in your home. This annoyance has now become a safety issue.

According to the National Fire Protection Association (NFPA), almost two-thirds of US home fire deaths happened in homes with no smoke alarm or no working smoke alarm.

The Nest Protect smoke and carbon monoxide (CO) alarm comes without that annoying chirp or the threat of false alarms. It's unique structure and settings give you quiet, visual low-battery reminders and allow you to relay to the alarm when the smoke is from that burning grilled cheese versus an actual fire. Its remote features also allow you to manage your alarm and receive alerts via your smartphone.

This innovative device gives you all the protection and security you need, without the annoyances. Get yours today at: https://nest.com/



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