ISSUE 6-9

# BITS & BYTES

INSIDER TIPS ON HOW TO USE TECHNOLOGY TO MAKE YOUR BUSINESS RUN FASTER, EASIER AND MORE PROFITABLY


IN THIS ISSUE



**September 2015**

***"TAG specializes in providing management level responsibility for all the technology in your business. This includes support for your network and working with other hardware & software vendors who's technology you use.***

***We do this with friendly, proactive & responsive service!***

**Joe Stoll, President**
Technical Action Group (TAG)

## Phishing Expeditions You MUST Make Yourself Aware Of

I hate to come across like a fear monger, but alas, these are the times we're living in. It's been some time since I've written about phishing (which has been around a long time), but as the phishing expeditions of cybercriminals reach a whole new level of sophistication and cunning to rob small business blind, I would be remiss not to bring it up again and educate you.

The word phishing comes from the analogy that Internet scammers are using email lures to 'fish' for passwords and financial data from the sea of Internet users.

Phishing, also called "brand spoofing"; is the creation of email messages and Web pages that are replicas of existing, legitimate sites and businesses. These Web sites and emails are used to trick users into submitting personal, financial, or password data. These emails often ask for information such as credit card numbers, bank account information, social insurance numbers, and passwords that will be used to commit fraud. The goal of criminals using brand spoofing is to lead consumers to believe that a request for information is coming from a legitimate company.

In reality it is a malicious attempt to collect customer information for the purpose of committing fraud.

### Warning signs - How to protect yourself

⇒ Do not reply to any email that requests your personal information.
⇒ Look for misspelled words.
⇒ Contact the financial institution immediately and report your suspicions.

### Variations That Will Rob You HUGE

One type of wire fraud currently targeting businesses is the Business Executive Scam (BES) which is a type of phishing. The potential victim receives an email that appears to come from someone of authority within the company (i.e. CEO, CFO). Fraudsters create email addresses that mimic that of others in the company. An email message will be sent to the CFO advising that the "executive" is working off-site and has identified an outstanding payment that needs to be made as soon as possible. The "executive" instructs the payment to be made and provides a name and a bank account where the funds, generally a large dollar amount, are to be sent. Losses are typically in excess of $100,000.

Technical Action Group Inc
TAG
we're I.T.

## Top 10 Cyber Crime Prevention Tips

**1. Use Strong Passwords**
Use different user ID / password combinations for different accounts and avoid writing them down. Make the passwords more complicated by combining letters, numbers, special characters (minimum 10 characters in total) and change them on a regular basis.

2. **Secure Your Computer**

**a) Activate your firewall.** Firewalls are the first line of cyber defense; they block connections to unknown or bogus sites and will keep out some types of viruses and hackers.

**b) Use anti-virus/malware / spyware software**
Prevent viruses from infecting your computer by installing and regularly updating anti-virus software.

**3. Be Social-Media Savvy**
Make sure your social networking profiles (e.g. Facebook, Twitter, Youtube, MSN, etc.) are set to private. Check your security settings. Be careful what information you post online. Once it is on the Internet, it is there forever!

Financial Industry wire frauds occur when Canadian financial institutions and investment brokers receive fraudulent email requests from what they believe to be an existing client. Unbeknownst to them, the email account of their client has been compromised. A request is sent by the fraudster to the financial institution/investment broker to have money transferred from "their" bank account usually to a foreign bank account.

This month alone, Presidents at 3 of our clients reported that members of their staff received emails from them to wire money. Thankfully, their staff spoke to these Presidents to confirm the instructions, which were found to be fraudulent.

Unfortunately not everyone is lucky enough to have such suspicion in their professional circles. Last week a client told me he knows someone who's accountant wired $75,000 of his client's money after receiving email instructions from his client—an email that turned out to be fraudulent. Are you wincing as much as I am?

**This Fraud Can Happen To ANYONE Unsuspecting**
**Learn The Warning Signs & How To Protect Yourself**

⇒ Beware of unsolicited emails from individuals or financial institutions presenting an urgent situation requiring immediate attention.
⇒ Prior to sending any funds or product requested by email, make contact with the sender by telephone to confirm that the request is legitimate.
⇒ Watch for spelling and formatting errors and be wary of clicking on any attachments, they can contain viruses and spyware.

### Phone number spoofing

If you receive a call and the call display shows a phone number of 123-456-7890 or 777-777-7778 (or any other strange combination of numbers), this is a phone number that has been programmed into the system so your call display indicates a different number than the originators. Although this does not mean the offer you are receiving is illegal, you should certainly have a "red flag" approach to any offer.

Why would a legitimate company try to obscure their identity?

### Automated dialers

The phone is ringing but no one is there when I answer.

Your phone may have a technical problem but you may also be receiving calls from an automatic dialer that logs the time the phone is answered. A telemarketer uses the information to indicate when a person will be at your number to answer the phone. For more information on Automatic Dialers you can research the CRTC web site.

### Unsolicited service calls - general services

Any false, deceptive or misleading promotion of services or solicitation for services. These scams typically involve third parties that make offers for telecommunications, internet, finance, medical and energy services. This category of scams may also include, but is not limited to, offers such as extended warranties, insurance and sales services.

If you have received an unsolicited telephone offer or a card in the mail you should use the "buyer beware" philosophy.

### Warning sign(s) - How to protect yourself

⇒ Credit card charges from foreign banks appearing on your statement ranging from $35.00 to $469.00.
⇒ Do you already have an existing warranty?
⇒ Have you checked with your car dealership?
⇒ How is the offer worded - does it make sense? Is it realistic?
⇒ Research on the internet.

## Unsolicited computer repair services

Generally, this scheme involves company representatives calling individuals and stating, for example, that it is Microsoft calling and that their computer is running slow or has viruses. They offer to repair the computer over the internet, which can involve the installation of software or the customers allowing the representatives remote access to their computer.

Recent variation being reported to the CAFC have involved the suspects identifying themselves as the Canadian Cyber Incident Response Centre and have taken a more aggressive approach with individuals by stating their computer is being used by hackers and that they will be held responsible if they do not allow the suspect to repair their computer.

Allowing a third party to download software or remotely access a computer carries inherent risks. Keyloggers or other malicious software could be installed to capture sensitive data such as online banking user names and passwords, bank account information, identity information, etc.

### Warning sign(s) - How to protect yourself

⇒ Unsolicited call representing computer repair-company (e.g. Microsoft) or indicating that it is the Canadian Cyber Incident Response Centre.
⇒ Caller requesting remote access to your computer or for you to view your event viewer.
⇒ Urgent solicitation indicating there is a threat to your computer.
⇒ Protect your computer with anti-virus software, spyware filters, email filters and firewall programs.

## Unsolicited vacation offers

Research the company with the Better Business Bureau and other sources from the internet.
If you have not requested information then "buyer beware" should be your thought process. Don't fall for a high pressure sales tactic, if it's a deal, it will be available again. If it is a prize you need not pay for it.

If your vacation call asks you to press a number like "9" or "5" it does not allow them to take over your residential line.

### Warning sign(s) - How to protect yourself

⇒ Some of the solicitations are valid, some are not.
⇒ Some offers are subject to you entering into a Timeshare agreement.
⇒ Some offer a high end vacation but reserve the right to change this location subject to availability.

## Unsolicited travel offers

By simply filling out a ballot to win a vacation at a home, boat or auto show, you may be set up for "suckers lists". Shortly after filling out this ballot, you may be contacted over the phone by someone claiming to offer you a "free" or "low cost"vacation. They will ask for your credit card number and personal information in order to hold the vacation for you, or they may request money in advance. **Don't give out your credit card information over the phone.** If you want to check out the value of these promises, seek out the advice of a legitimate travel agency in your area. If you have provided credit card information to the telemarketers, be aware that most companies have policies that allow you to cancel your reservation within 30 days. **Do not let anyone pressure you into committing.**



**...Prevention Tips Cont'd**

**4. Secure your Mobile Devices**
Be aware that your mobile device is vulnerable to viruses and hackers. Download applications from trusted sources. Password protect your device with a strong password.

**5. Install the latest operating system updates**
Keep your applications and operating system (e.g. Windows, Mac, Linux) current with the latest system updates. Turn on automatic updates to prevent potential attacks on older software.

**6. Protect your Data**
Use encryption for your most sensitive files such as tax returns or financial records, make regular back-ups of all your important data, and store it in another location.

**7. Secure your wireless network**
Wi-Fi (wireless) networks at home are vulnerable to intrusion if they are not properly secured. Review and modify default settings. Public Wi-Fi, a.k.a. "Hot Spots", are also vulnerable. Avoid conducting financial or corporate transactions on these networks.

# Succession Planning
# What Will Happen To Your Business?

Succession planning requires careful thought and consideration.

Here are just a few key points and questions from Douglas Pinnell's talk at the OAA Conference in Hamilton earlier this year.

## What Is The True Value Of Your Business?

The value of your business is based on 3 factors;

1, Does someone want to buy it?
2. What are they willing to pay for it?
3. Are they financially able to pay for it?

There are different valuation formulas that can be applied based on a multiple of your earlies + a value for fixed assets + a value for the "Good Will" of your business. However, the true value comes down to what someone is willing and able to pay for your business.

## Who Should You Sell Your Business To?

When you are ready to leave your business, there are 3 succession options:

1. Close the business.
2. Sell to an external buyer.
3. Sell internally.

A merger may be considered a fourth option, although it is really a variation of the second and third options depending on the parties involved. Selling externally usually offers the benefit of an up front cash payment, but ofen includes a requirement of several years of service during the transition period. Do you want to continue working for several years? And can you handle being assimilated into the new owner's way of doing business?

On the other hand, an internal sale involved identifying the right candidate to take over your leadership role. Do you have a STAR within your business who would be an appropriate choice?

A S.T.A.R. is an internal candidate who may seem *Scary,* and/or *Threatening,* but whom is also *Amazing* for your business and is likely the *Right* choice. Have you groomed a STAR? Do they know that they are part of your succession plan?

# Establishing A Buy/Sell Agreement

If your business is structured as a partnership or corporation, it is very important that you have an agreement outlining the rights of owners or shareholders. There are 4 dimensions of a buy/sell agreement that should be included (The 4 D's)

1. Disagreement / Departure. 2. Debt / Divorce 3. Death 4. Disability / Disease

The specifics of the 4 D's will vary depending on the structure of your business and the needs or desires of the owners. Have you created your buy/sell agreement?

Call Douglas Pinnell at Mumby Insurance Brokers for Help today!
1-800-446-4745. http://mumby.com/

Info@TechnicalActionGroup.com **http://www.TechnicalActionGroup.com** 416-489-6312

**...Prevention Tips Cont'd**

**8. Protect your e-identity** Be cautious when giving out personal information such as your name, address, phone number or financial information on the Internet. Make sure that websites are secure (e.g. when making online purchases) or that you've enabled privacy settings (e.g. when accessing/using social networking sites).

**9. Avoid being scammed** Always think before you click on a link or file of unknown origin. Don't feel pressured by any emails. Check the source of the message. When in doubt, verify the source. Never reply to emails that ask you to verify your information or confirm your user ID or password.

**10. Call the right person for help** Don't panic! If you are a victim, if you encounter illegal Internet content (e.g. child exploitation) or if you suspect a computer crime, identity theft or a commercial scam, report this to your local police. If you need help with maintenance or software installation on your computer, consult with your service provider or a certified computer technician.

For more information on helping children protect themselves while on the Internet, visit: Cybertip.ca