

A Critical Look at Privacy and Security

October 11, 2003

Robert Gusnowski

With the start of Science and Technology week (October 10-14) it is good time to stop and reflect on the issues of privacy and security. It is a good time because while technology is a useful and powerful tool when used appropriately, it is also a useful and powerful tool when used for illegitimate purposes.

One item up front - security. There is no such thing as a totally secure system. Security can only be managed. A balance between ease of use, cost of use and total effectiveness must be maintained. Too much security and users will find ways to bypass the system. Not enough security and we can be considered liable for not taking reasonable precautions to ensure the protection of confidential information.

Second item up front - people are the weakest link in the chain. In World War II there were several key events that helped crack the code that the Germans were using (The Enigma Machine). While mathematicians laboured to solve the problem they were helped by simple human weakness - human error was and likely always will be a point to consider in considering the issues of security and privacy.

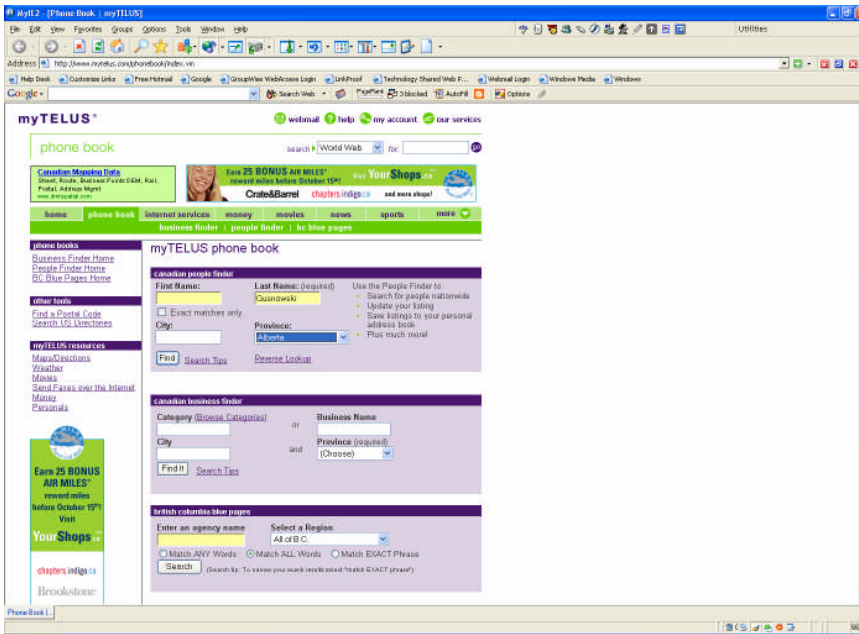
The Internet and Privacy

Consider for a moment the power of the internet - at your fingertips is more information than was ever available to mankind at any other point in time. Information on every subject from esoteric philosophy to cold hard physics can be found easily and quickly. Of course one must consider the source of the information: it may be factually correct or it may be complete fiction. Nonetheless the critical individual can glean a massive amount of factual correct information in a very short period of time.

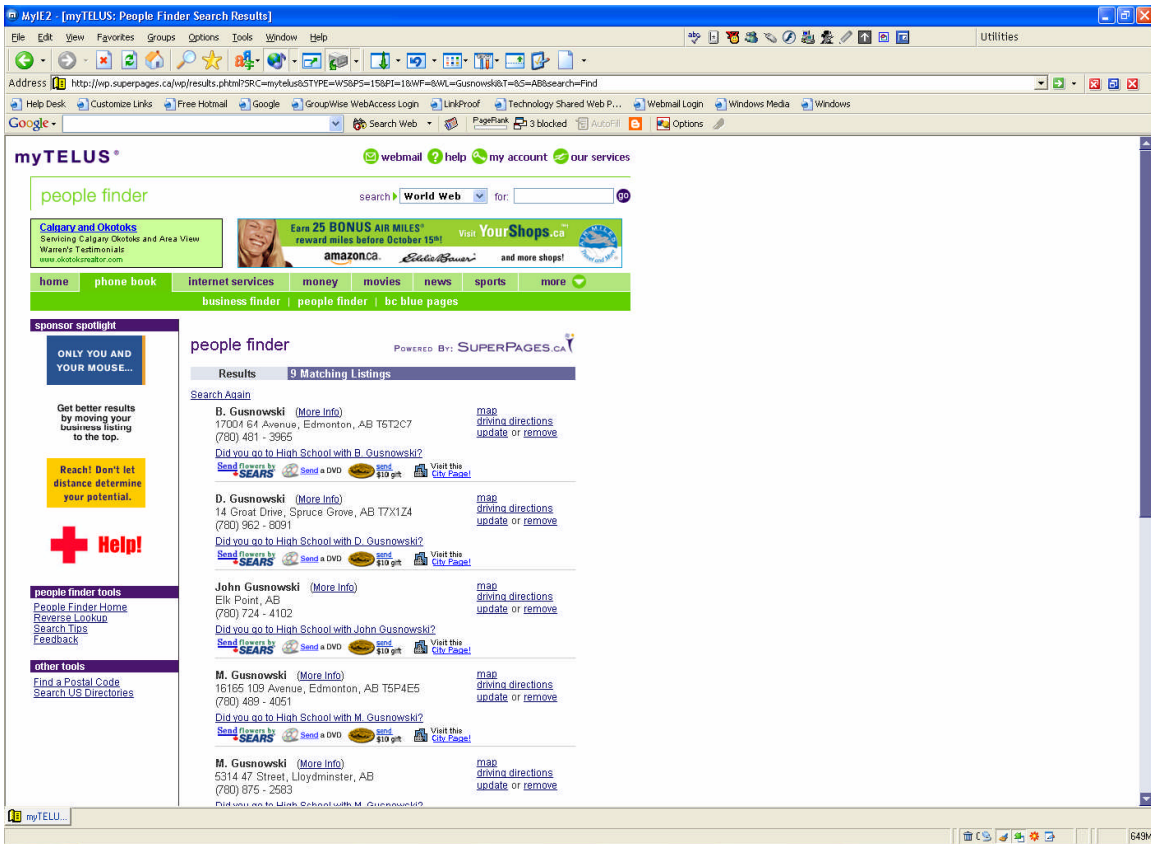
Take a minute to explore the power of the internet.

Imagine this scenario - you want to find about all the Gusnowski's that live in the province of Alberta. *(as a complete aside – the only reason I am using my family name here is because the amount of information that I am going to show you here is well beyond the scope of what any normal person would want revealed)*

Our first stop is to go to the public phonebook at <http://www.mytelus.com/phonebook/index.vm> and search for all the Gusnowski's in the Province of Alberta.



All that I have put in is the last name Gusnowski and I have limited the search to the Province of Alberta.



The search results show that there are nine Gusnowski's listed in the province.

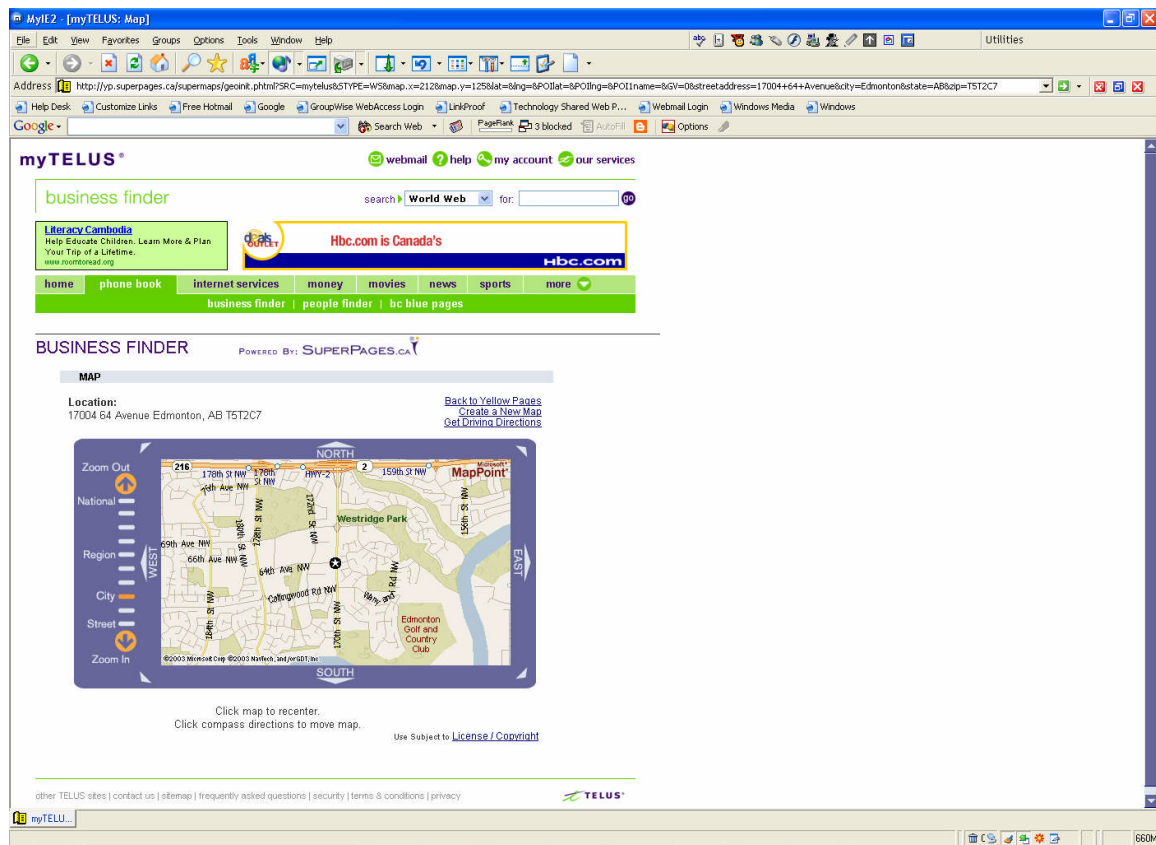
I just happen to know that all of the Gusnowski's are related so I am going to use the information to find a cousin I have not seen in probably twenty years – Brent Gusnowski.

There is a B. Gusnowski listed. In a matter of seconds I learn that he lives in Edmonton at 17004 64 Avenue, Edmonton, Alberta, postal code T5T 2C7, and that his phone number is (780) 481 – 3965.

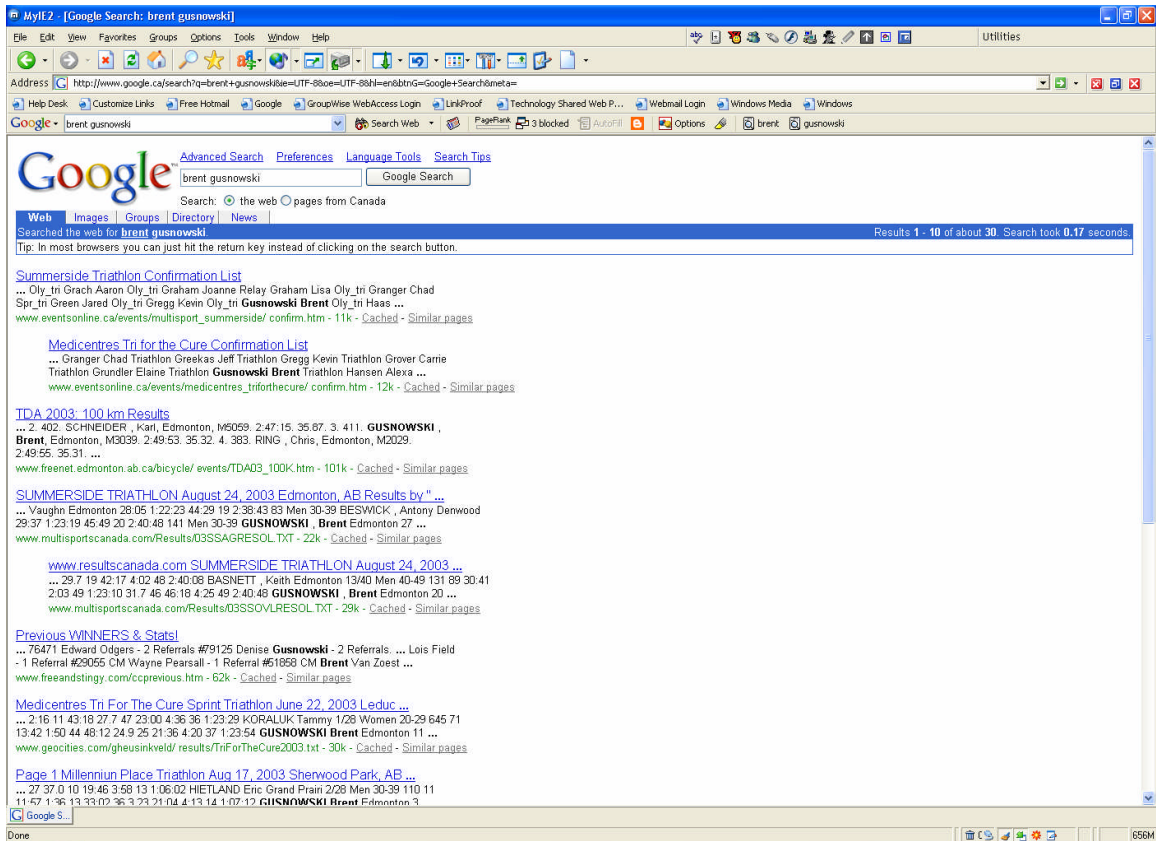
As an aside - if only the postal code was provided – as in some listings – I could go to Canada Post's website and use the reverse lookup tool

<http://www.canadapost.com/tools/pcl/bin/range-e.asp> to narrow the search down to part of a city block.

If I don't know Edmonton, Telus is kind enough to even offer me a map.



Our next stop is Google – this search engine can reveal a host of information about many things. It is quite amazing the path we humans leave behind during our short journey on this earth and now, thanks to the internet and the power of Google we leave a path for any mere mortal to easily find and trace.



Within a fraction of a second I find that Brent participates in many sporting events. The first listing is for the Summerside Triathlon.

I won't bother to go on, but you can easily see how quickly information can be found.

If we shift our focus off of the legitimate task of finding a “lost cousin” and over to the idea of a pedophile attempting to track a child we can see how quickly this ease of access becomes a nightmare. There are other more illicit ways to gather information on the internet that I would prefer not to reveal in the course of this document, but if I know about them you can rest assured that those with less honourable intentions do also.

Protecting Our Privacy

What can we do to protect our privacy both on the internet and in general life? The answer lies in two words – privacy and security.

We start by **being aware** of how and when we give out personal information. The next step is **being assertive** when asked for information you do not feel is necessary – ask questions and know why information is being requested. Last is **being and advocate** for our own privacy rights – privacy is too big an issue to rely on others we must take personal responsibility for ensuring that our privacy is protected.

The Crime of Identity Theft

This is currently a big an issue and it must be given separate consideration. The crime of identity theft is on the rise. Using a variety of methods, criminals steal Social Insurance numbers (SIN), driver's license numbers, credit card numbers, ATM cards, telephone calling cards, and other pieces of individuals' identities such as date of birth. They use this information to impersonate their victims, spending as much money as they can in as short a time as possible before moving on to someone else's name and identifying information.

There are two types of identity theft. "Account takeover" occurs when a thief acquires your existing credit account information and purchases products and services using either the actual credit card or simply the account number and expiration date. "Application fraud" is what some experts call "true name fraud." The thief uses your SIN and other identifying information to open new accounts in your name. Victims are not likely to learn of application fraud for some time, because the monthly account statements are mailed to an address used by the imposter. In contrast, victims learn of account takeover when they receive their monthly account statement.

It is an unfortunate reality that you cannot prevent identity theft. Criminals can commit identity theft relatively easily because of lax credit industry practices and the ease of obtaining SINs. But you can reduce your risk. There are a few simple practices that can help minimize the risk of identity theft:

1. minimize the amount of information a thief can steal, do not carry extra credit cards, your Social Security card, birth certificate or passport in your wallet or purse, except when needed
2. if possible, do not carry other cards in your wallet that contain the Social Security number (SSN), except on days when you need them
3. install a locked mailbox at your residence to deter mail theft
4. when ordering new checks, pick them up at the bank - don't have them mailed to your home
5. reduce the number of credit cards you actively use to a minimum - carry only one or two of them in your wallet - consider canceling unused accounts

This is by no means a complete list but rather a few simple common sense suggestions. For more information about identity theft visit the Government of Canada website http://www.privcom.gc.ca/fs-fi/02_05_d_10_e.asp and be aware that there are also illegitimate companies out there that use the threat of identity theft to sell you un-needed and sometimes expensive services. When in doubt always refer back to trusted sources such as the government or other known reliable organizations.

The Internet and Network Security

When was the last time you changed your password? Is your password easy to guess? Can you be sure you are the only person that knows your password?

In the world of the internet and computers your password is the key to your identity. Just as you would never indiscriminately share the keys to your house or car with perfect strangers, so also should you never share your passwords.

A point to ponder – a password of less than eight characters or a password that is based on a word that can be found in the dictionary can be “cracked” using brute force guessing techniques (utilized by many free and readily available hacking tools) in less than 5 minutes on an average computer.

Just as there are some practical ways to prevent identity theft there are some easy common sense and practical ways to protect yourself while using computers and the internet.

Of the tools we most often rely on e-mail is probably one of the most open to abuse. We see viruses being propagated by email, SPAM filling our mailboxes and not commonly recognized is the fact that e-mail is by its nature less than secure.

E-mail should always be considered as a semi-private means of communication. It can be viewed as being similar to a postcard in that it can be read by any individual (or computer system) that can “intercept” the message along its path from sender to receiver. One point to consider, however, is the mere volume of e-mail and the speed of today’s mail servers and networks makes this a less than practical task. Unfortunately that is no guarantee of security – it takes little programming skill to write a “sieve” program to **intercept** interesting e-mail messages that contain key words such as *credit card, phone number, money* or countless others that may make interesting reading: while there may be too many messages to read them all there are ways to separate the interesting from the mundane.

Simple common sense ideas can help eliminate the risks. If a message is sensitive write the message as an MS Word Document, password protect the document and send it as an attachment to your e-mail message. It is much more difficult to intercept a password protected attachment. Put your brief message in the e-mail itself and keep the details in an attached document. This requires little effort and it can add an extra layer of security.

A second suggestion is to have more than one e-mail address. The GroupWise mail system that is used within Buffalo Trails is neither actively monitored (although it is scanned for viruses, SPAM and content keywords) nor has it been restricted for personal use. In the corporate workplace, however, this is becoming the exception rather than the rule: many organizations now restrict personal use of corporate e-mail systems.

Getting and addition e-mail address is quite easy as there are many free e-mail services available as well as low cost (more reliable) e-mail services on the internet. A suggestion is to have three e-mail addresses:

- A primary business e-mail address for work

- A personal primary e-mail address for all other correspondence

- A third **JUNK** address for shopping and online forms

By utilizing a *JUNK* e-mail address you can minimize the amount of SPAM that ends up in your personal or corporate e-mail account. When shopping or filling (non-government or other “critical” forms) use your JUNK e-mail account so that if the e-mail address gets sold or used on a mailing list the SPAM doesn’t get sent to your more legitimate e-mail account(s).

On our corporate network (Novell and GroupWise) identities and access are an issue. GroupWise is unique in that it is easy to identify whether an e-mail message was actually sent from a user’s e-mail account or forged from another outside source. This is not the case in all e-mail systems. On our central office and school networks we have sensitive and confidential information. That information must be secured.

Have you ever seen a computer workstation in your school (or in central office) that was *logged in* the network but the machine was left unattended? What would be consequence be if someone sat down at the unattended workstation and found out the address (or other confidential information) of a child? We must be actively vigilant in keeping our network security intact – again the human factor is the weakest link.

Keep your password secure and change your password often are the two most repeated pieces of advice that can be given. At the network level we can lock down the system to force these two actions (*forcing periodic password changes and password length restrictions*) but there is a reality in that if security restrictions are impacting *end user ease of use* then end users will often find ways to circumvent the security. Forcing a user to have a 10 or 12 character password only to have them use a pencil and write password on to the bottom of they keyboard is not enhancing security in any way!

Your password is what tells the computer that you are who you say you are so protect your password. Here are a few ideas to help you do just that:

1. first and foremost, NEVER give your password to anyone
2. make your password something you can remember - do not write it down - if you really, honestly forget your password, we can easily give you a new one -we'd rather set your password once a month because you forgot it than have someone find it written down and gain unauthorized access to your account
3. make your password difficult for others to guess
4. think along the lines of the license plate rule: take a phrase and try to squeeze it into eight characters, as if you wanted to put it on a vanity license plate
5. words like “foobar”, “xyzy” and “qwerty” are still just plain **BAD** words - they are also popular passwords, and the crack programs look for them - avoid them

The reality is that the *genie is out of the bottle* – technology is a part of our lives. Each scientific advance drives technology deeper into all aspects of our life. Our world is changing but change has happened before and we as humans are exceptionally good at adapting to change. There is no reason to panic but we need to be aware of the risks, the issues and the ways that we can protect ourselves, our students, and how to evolve and adapt to these changing times.

LINKS

Free E-mail Services

MyRealBox <http://www.myrealbox.com>

Fastmail <http://yoursite.gr/fastmailgr/login/index2.htm>

Hotmail <http://www.hotmail.com>

Free E-mail Address Directory <http://www.emailaddresses.com/>

Security and Privacy

Privacy Commissioner of Canada http://www.privcom.gc.ca/fs-fi/02_05_d_10_e.asp

Government of Canada Internet Guide http://www.cio-dpi.gc.ca/ig-gi/i-mo/sp/sp_e.asp

Passwords and Network Security

NIST Computer Security Center <http://sbc.nist.gov/cyber-security-tips/800-12/ch16/chapter16.html>

MIT Guidelines for Choosing a Password

<http://web.mit.edu/is/help/network/passwords.html>

Other / General

A quick guide to email security <http://www.zzee.com/email-security/>

Activist: Guide to Email Security <http://www.activist.ca/guide/encrypt.html>

Netsys <http://www.netsys.com/>

CISSP <http://www.cissps.com/>