BLOOM MICROTECH
Discover Real Service

FROM BEHIND THE SERVICE COUNTER

So you've survived the holidays, now don't get caught by these scams…

Everyday it's getting harder to stay ahead of the internet scammers. It seems the web has become fertile ground for all kinds of tricksters and they aren't just playing practical jokes. Here's some quick tips on how to become cynical in your old age…

EMAIL SCAMS:
a) If you open an email and all you see is a link, DO NOT CLICK ON IT. They want you to, to just to see what it is and… that'll cost ya'!
b) Anyone addressing you as "dearest" or "friend" or starts a familiar conversation but you don't recognize the sender, chances are they don't know you. Not to be trusted!
c) Too good to be true… You've just won the Irish Sweepstakes, your email was submitted and you've won, some else won and wants to share their winnings with you? Yup! IT'S NOT TRUE.
d) Are you that important that the Who's Who of something that sounds official really wants to list you? I'm not either.
e) Dead relatives that you don't know just don't exist. And just how did the "solicitor" find you anyway? Sorry, no fortune to be inherited here.
f) The Nigerian letter moved from snail mail to the internet and now everyone is trying to move a fortune of ill gotten gains out of some bizarre country and wants you to share, just for helping them by setting up a bank account.
g) Your friend is not stranded somewhere and needs you to send money via Western Union. WU does not require legitimate ID to collect funds so if you think your grandchild needs money quickly, it probably is a hoax.

INTERNET SCAMS:
a) Looking for the FREE utility to fix your computer? Trust us, it isn't going to be free by the time you finish with it.
b) For that matter, almost anything that's free isn't really. Quite often advertising portals are opened up or email and identity data gathering is done this way. Be ready for a lifetime of spam unless you don't care about changing your email address often.
c) Software cannot speed up your computer any faster than it is physically built for. That should be obvious but time after time we see "speed enhancers" installed that actually slow down the system while they process spam.
d) Having fun surfing the web when suddenly the Police show up on your computer, indicate that you've been apprehended surfing porn and downloading illegal music and if you don't pay the $40 fine immediately your computer will be seized? Well part of this scam is real! This is called a hijacker because it hijacks your computer and you can't use it until something is done. By the way, as you suspected, this is not the Police even though the page has pretty pictures of the RCMP and even the Governor General. The

really "good" one snaps a picture of you with your webcam and threatens that they now have picture evidence of who committed this heinous crime.
If you do pay, they'll free up your system but expect to see them back next month…

GENERAL STUFF:
Hackers aren't randomly interested in your computer but they do love collecting email addresses to sell to the spammers. The firewall that comes with Windows is often enough to keep the average hacker out but if you are seriously targeted for national secrets, Swiss bank account numbers or intellectual corporate property chances are you're going to need serious protection beyond the scope of the average end user. Keep your requirement for security in perspective.

You're more likely going to be susceptible to the "Windows Support Team" (or something official sounding like that) who call you at home to report that your computer is running slow because you're got a virus and they can help. These guys are very convincing and many trusting users have given them remote access to their computers over the internet. Now it gets interesting… First they claim to tune up your system and that they can continue the service for around $250 a year if you give them your credit card number (by now you should be getting uncomfortable but you'd be surprised at how many call recipients don't). Of course they have done nothing but now they have your card number. We know of one client whose bank thwarted an attempt to charge $5,000 to her card before their security dept caught and shut the transaction down. Secondly, we are unable to determine precisely what they have done to your computer so a complete reload is immediately required. AND if you use your computer for on-line banking we further suggest you replace all access passwords and credit cards asap.

The real problem is that all these wild and crazy schemes continue on. That means that they work and that poor unsuspecting souls are falling for them.

Please be careful out there!

Harley Bloom
Bloom MicroTech