Safe Computing

Avoiding Unpleasant Surprises from Scams, Malware and Phishing

Roy Blake, Feb. 2014
The Basics

• Backup
  – A backup of all your documents means you can recover your digital life, even if your computer is hopelessly trashed.
    • Best to use at least two methods
      – For example, Windows backup or Apple Time Machine AND Dropbox
  – Backups also protect your data in case of hardware failure.
  – Simplest method for documents is to copy to a USB key.

• Updates
  – Keep important programs up to date, automatically if possible.
    • Operating system
    • Browser
    • Office, Acrobat reader, Java, Flash player
More Basics

• Passwords
  – OK to use one password for a number of unimportant sites.
    • Example: comments on blogs or websites
  – Each important site needs its own password.
    • Examples: banks, credit cards, email accounts
  – Don’t use common words or sequences that are easily guessed.
Most Common Passwords

As recently stolen from Target. Don’t Use These!

• password
• 123456
• 12345678
• qwerty
• abc123
• monkey
• 1234567
• letmein
• trustno1
• dragon
• baseball
• 111111
Passwords

• Words in dictionary are easily guessed.
• Arbitrary sequences are hard to remember.
• OK to write down passwords and keep in wallet (preferably not taped to your monitor!)
• Programs like Password Safe are available to store passwords securely.
• Don’t give out passwords.
  – Banks, etc., will not ask for them in emails, make sure you really are on their website before entering.
personal

- Gmail Roy [roy.blake]
Clear Clipboard

Pressing OK will copy the password of the selected item to the clipboard. The clipboard will be securely cleared when Password Safe is closed.

Pressing Cancel stops the password being copied.

☐ Don't remind me again

[OK]  [Cancel]
Antivirus Software

• Essential with Windows, advisable with Macs, probably unnecessary with Linux.
• Don’t rely on the software that comes with Windows (do use the firewall though.)
• Available for smartphones/tablets, opinions differ on how necessary.
• I like Avast! (free version)
• Windows Security Essentials also seems ok but not for Win 8.
• Make sure you keep it up to date and running all the time.
• No A/V software is perfect, keep your eyes open as well.
Malware

• Generic term for harmful software
  – Viruses
    • Harm computer, delete files, send your data to others, etc.
      – Sometimes combined with extortion attempts (“Scareware”)
  – Trojans
    • Take over computer, often to use it for sending spam, etc.
    • Often these are unnoticed by the user.
  – Worms
    • Spread from computer to computer over internet.
  – Unwanted Toolbars, Home-page switching, etc.
    • Can send browser to addresses not what you intended.
How Malware Spreads

• Drive-by Downloads
  – Hard to avoid — why you need an A/V program and updated software.

• Click-by-Accident or Misdirection Installs
  – Don’t open attachments unless you are expecting them and know the source.
  – Read everything before you click.
  – Make sure the program really is what you think it is.
  – When Windows asks if you want to allow a program from an unknown source to run, think carefully before agreeing.

• Infected documents
Let's be having youbaby. This is **Pennie**.

I found your profile via facebook. I was excited! You're cute! I want to share some hot photos with you, babe! Got big boobs, and a big butt... and know how to use them :)

Click bellow to view my (18) private photos:  

[**Pennie's pics**](#)
avast! Web Shield has blocked a harmful webpage or file.

Object: http://.../?kv=Martina
Infection: URL:Mal
Process: C:\Program Files (x86)\...\firefox.exe

More details...

Report the file as a false positive
Checking Websites for Safety

• Any website can be hacked and turned into a malware distributor.
• Google flags websites where it finds malware.
• Anti-virus software will also warn about dangerous sites.
• When looking for software, watch out for look-alike names and sites.
• Look for https:// not http:// on banking sites etc.
• Ordinary sites may give errors if you use https://
February Lunch
January 8, 2014 by roygblake

Our next lunch is Wednesday, Feb. 5 at Club Canri in Thorold. This lunch will be
This Connection is Untrusted

You have asked Firefox to connect securely to retirees.niagaracollege.ca, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Get me out of here!

- Technical Details
- I Understand the Risks
Wi-Fi

• Be sure your router uses encryption and don’t use the default password.
• Most public Wi-Fi sites are not encrypted so anyone within range can see your traffic with special software.
• Even if they are encrypted, anyone else who is logged in can see your traffic with special software.
• Don’t use public Wi-Fi for anything involving logins or confidential data unless you are using an encrypted connection (https not http) or a VPN.
• Make sure to connect as “public network.”
Password Sniffer

Capture passwords through web pages(http), email(smtp, pop3), ftp, telnet.
E-Mail Scams

• Use “Social Engineering” to fool you into doing something you soon wish you hadn’t.
  – Phishing: Obtains credentials by fraud.
  – Advance-fee or “419” scams extort money by promising more money later.
  – Money-mule offers: money laundering.
  – Fake job offers cost you money when you thought you were going to get paid.
  – Fake distress emails have you send money to a “friend” who turns out not to be so friendly.
Phishing

• An email or website pretends to be something it’s not.
  – Your bank.
  – Your email provider.

• Stop this by remembering:
  – No one will ask for your password in an email.
  – Never go to any important site by following a link in an email.
    • Enter your bank address directly in your browser.
You have exceeded the limit of 10 GB storage on your mailbox set by Service/Administrator, and you will be having problems in sending and receiving mails Until You Upgrade Your Mailbox.
Click the link Or copy paste the link and fill out the information to upgrade your Mailbox.: http://serviceemailhelpdesk.webs.com
Hello,

Here is an important document that I want you to see. I tried sending it directly here but did not deliver so I had to use my Google Drive. Please see the document and sign up with your personal e-mail to open the document.

[Open here]

Thanks.
Authorization required to view this document - Select your email provider and Sign In by your Email and Password!
From: CIBC Card <service+rih977jsk442@berkshirerlakesrealestate4sale.com.com>
Date: February 8, 2014 1:26:31 PM GMT-05:00
To: jpblake@cogeco.ca
Subject: [SUSPECTED SPAM] Important Notification
Reply-To: CIBC Card <service+rih977jsk442@berkshirerlakesrealestate4sale.com.com>

Dear CIBC valued customer,

Due to maintenance services on our databases, we require our customers to verify their online accounts by completing an online form.

We have upgraded our services to provide a higher layer of security to our clients.

To verify your online account click on the following link to access the validation form:

Click here to login to your account
Your credit card has been used through this IP Address 41.249.88.122 in Morocco

If it has not been used by you, please change your password and lock transaction by clicking here
Other Phishing Attacks

• Twitter
  – Direct message from account you are following either sends you to a spam link or asks for login
    • Don’t follow people you don’t know.
    • Watch out for fake celebrity accounts.

• Text messages on cellphones
  – Send links or try to start exchanges with random numbers.
  – Just ignore messages from anyone you don’t know.
“419” Scams

• So named after a section of the Nigerian criminal code prohibiting fraud.
• Not all come from Nigeria.
• Promise to give you a lot of money if you work with them, which soon involves sending money upfront.
• Stop these by remembering:
  – You haven’t won a million dollars in a lottery you didn’t enter.
  – No one is going to give you a million dollars for doing a little work.
Hello Partner,

My name is Sheryl Van Der Hoff and I work in Nedbank South Africa and am the account officer of late Nelson Mandela, and there is a deposited funds of $880,000 United states dollars in our bank that was not mentioned in his Last Will Testament which was announced openly to South Africans today 03/02/2014.

This funds has been dormant since february 2010 which was deposited before the 2010 World Cup hosted here in South Africa. I am looking for your trust and honesty to transfer the said funds into your bank account in the states, then we can share with a 70/30 percentage ratio.

Please urgently get back to me as soon as possible if I can be able to trust you in this so I can provide you with details on how to transfer the funds into your account.

Thanks

Account officer in charge
Nedbank South Africa
Mrs. Sheryl Van Der Hoff
I am in the military unit here in Afghanistan, we have some amount of funds that we want to move out of the country. My partners and I need a good partner someone we can trust. It is risk free and legal. Reply to this email majoralanedward07@admin.in.th
Sincerely
Major. Alan Edward
Happy New year,

Mark and my wife Cindy Hill Missouri won a Jackpot we have decided to donate the sum of $1.5 Million USD to you. Contact us via our personal email for more details (cindy-hill@qq.com) You can verify our story by visiting the web page below. http://www.huffingtonpost.com/2013/02/25/missouri-powerball-winner_n_2749795.html fill the following. 1.Name 2. Country 3.Sex Note that you have to contact my private email for more informations (cindy-hill@qq.com).

Goodluck,
Mrs Cindy Hill
Money-Mule Offers

- An email from a supposed company offers you a job processing payments and sending them to head office
- Used to launder money obtained by other scams
- Often the email links to a real company website (but the company has nothing to do with the scam)
- Avoid by knowing:
  - No legitimate business is going to hire you just to move money from one account to another.
Impex Consult Financial Consulting Group was established early in 1994. The group's offices are located in over 20 countries of the world. The Group comprises a consultancy, a legal, an auditing and an appraising companies. All the companies controlled by the Impex Consult holding pursue one ultimate goal - that of improving efficiency of the client’s business.

Impex Consult is one of the oldest companies on the market, with invaluable experience of working with investments. We are proud of the trust our clients and partners have put in us. The core of our success is our specialist team. We are constantly developing and always keen to bring more determined and ambitious professionals into our team. At this stage, we offer you to start your career in our team as a Transactions Specialist.

The duties would involve prompt processing of incoming cash funds and their transfer to accounts indicated by our managers. With efficient time management, your whole day’s work should take 3 to 5 hours.

What we expect from a candidate
- Higher (tertiary) education
- Age upward of 20
- Experience of handling money remittances (appreciated)
- Knowledge of principle electronic payment instrument
- Confident computer skills

What we offer
- Speedy career progress
- High earnings plus performance result bonus

follow this link to take a visit to our web site
Job Offers, Get-Rich Quick Advice

- An email offers to hire you to “work at home”
  - You need to send money for a starter kit
- An email offers you the secret of making lots of money on the internet
  - You need to buy a book, video etc.
  - The book may tell you that the way to make money is to sell lots of the books online!
- To avoid:
  - Know that no one is going to offer you a job out of the blue. Especially one that pays really well!
“Secret Shopper” Scam

• Variant of the job offer scam
  – You are offered a job as a secret shopper
  – One of the assignments is to send money by Western Union or similar
  – They send you a cheque that more than covers the amount and you keep the rest.
  – You do it and then the cheque bounces.

• To avoid:
  – Legitimate companies won’t offer you a job out of the blue. You go to them, and they pay you a reasonable rate, after you do the work.
Greetings,
This is an official request from shopper's guide seeking for serious individuals who will work as a secrete Shopper in your region in Canada and earns up to $150.00 per hour. Get back to us by calling our telephone number or send us an e-mail if interested.
Respectfully,
Tim Williams
Tel: 647-909-0998
E-mail: timwilliams011@gmail.com
Fake Distress Emails

- You get an email from a friend who claims to be in trouble in a foreign country
- You are asked to send money
- Usually the friend’s real email address is used
  - Their account has been hacked, usually by a phisher
- To avoid
  - Notice lack of details, names, etc.
  - Inconsistent style compared to your friend’s
  - If tempted, first get in touch with your friend some other way (phone, another email address, knock on their door) or check with a mutual friend
Hello,

I'm writing this with great grievance, My family and I came down here to Manila, Philippines on a short vacation, Unfortunately we were mugged at the park of the hotel where we stayed, All money, credit card and cell phones were stolen away from us, luckily for us we still have our passports. Our credit cards can't be charged by the hotel as we already reported it as a stolen card and the card company had canceled it, we can only get a new one when we make it back home safely.

We've been to the Embassy and the Police but they're not helping issues at all, Our return flight leaves soon, we're having problems settling our hotel bills and the hotel manager won't let us leave until we settle the bills. We are really freaked out here and we really need your financial assistance, I promise to reimburse you as soon as we return back home. Please let me know what you can do to help so i can proceed by giving you all the details needed in getting the funds to us here via Western Union or Money Gram.

Kindest Regards.
Computer-repair Scams

• Often use phone call to start.
  – Call is supposedly from your computer company, or Microsoft, etc.
  – Says they can see you have a problem with your computer.
  – Offer to take control of it and fix it.
    • You give them control following their instructions.
    • They get as much money as they can while deleting your files.

• To avoid:
  – Sorry, Microsoft doesn’t care about you!
  – Just hang up on such calls.
“Scareware”

• Similar to above but scarier.
  – You are informed by a pop-up message (from a website) that you have viruses.
  – A scarier version supposedly comes from the cops and may lock your computer.
  – You have to pay to make the problem go away.

• To avoid:
  – These are always scams: Do not pay.
  – If the cops really want you for something serious, they won’t notify you by computer message first!
You have viruses on your computer

We have magically detected viruses on your computer from your web browser.

The only way to remove them is to install our nominally priced software right now. Act now before you realize this is a scam.

Files scanned: 4,523  Viruses found: You don't want to know

YES  I trust you, random website
**ATTENTION!**

Your computer has been blocked for safety reasons listed below.

You are accused of viewing, storage and/or dissemination of banned pornography (IMZ pornography/snapka/vape etc). You have violated World Declaration on non-pornographic of child pornography. You are accused of committing the crime envisaged by Article 161 of Canada criminal law.

Article 161 of Canada criminal law provides for the punishment of deprivation of liberty for terms from 5 to 61 years.

Additionally, you are suspected of violation of "Copyright and related rights Law" (downloading of pirated movies, videos, songs) and of use and/or dissemination of copyrighted content. Thus, you are suspected of violation of Article 146 of Canada criminal law.

Article 146 of Canada criminal law provides for the punishment of deprivation of liberty for terms from 3 to 7 years or 150 to 550 basic amounts fine.

It was from your computer, that unauthorized access had been made to information of Ukraine importance and to data stolen for public interest access.

Unauthorized access could have been arranged by yourself purposely or necessity motives, or without your knowledge and consent, provided your computer could have been affected by malware. Consequently, you are suspected - until the investigation is held - of innocent infringement of Article 215 of Canada criminal law ("Law on negligent and reckless disregard of computers and computer aids").

Article 215 of Canada criminal law provides for the punishment of deprivation of liberty for terms from 5 to 6 years and/or up to CAD $500,000 fine.

Further, after information of your personal computer was examined, it was found out that your personal computer had been regularly used for bulk-spamming, either arranged by yourself purposely or necessity motives, or without your knowledge and consent, provided your computer could have been affected by malware. Bulk-spamming is a way to disseminate material of banned pornography. Consequently, you are suspected - until the investigation is held - of innocent infringement of Article 301 of Canada criminal law ("On bulk-spamming and malware (Virus) dissemination").

Article 301 of Canada criminal law provides for the punishment of deprivation of liberty for terms up to 3 years and up to CAD $250,000 fine.

Warrants, made that both your personal identifiers and location are well identified, and criminal case can be opened against you. In course of 96 hours it is necessities of citizens per above arrests. Criminal case can be submitted to court.

However, pursuant to amendments to Canada criminal law dated July 15, 2013, and according to Declaration on Human Rights, your disregard of law may be interpreted as an unintended (if you had no intentions thereof) and no punishment will follow. However, it is a matter of whether you have paid the fine to the Treasury to the effect of initiative aimed at protection of cyberspace.

The penalty set must be paid in course of 48 hours as of the breach. On expiration of the term, 48 hours that follow will be used for automatic collection of data on yourself and your surroundings. Criminal case will be opened against you.

**Amount of fine is CAD $100. You can pay a fine using Kash vouchers.**

As soon as the money arrives to the Treasury account, your computer will be unlocked in course of 24 hours.

Thus, in 7 days term you should remove the breaches associated with your computer. Otherwise, your computer will be blocked up again and criminal case will be opened against yourself (with no option to pay fine).

Please mind, that you should enter only verified pass of vouchers and amounts from cashing out of vouchers once used for fine payment. If erroneous pass were entered, or if attempt was made to cancel vouchers after transaction, then, apart from above breaches, you will be charged with fraud (article 377 of Canada criminal law: 1 to 3 years of imprisonment) and criminal case will be opened.
“Ransomware”

• You get a popup that says all your files have been encrypted and you have to pay to regain access.

• Virus is often installed by downloading a “fake jpg”.
  – Something like: barenakedlady.jpg.exe

• Solution:
  – Do not pay any money! They may leave your files encrypted anyway.
  – You may be able to remove the program with A/V software but that won’t decrypt the data.
  – Restore data from backups (you DO have them, right?)
Your personal files are encrypted!

Your important files encryption produced on the computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key XMK2013 generated for the computer. To decrypt files you need to obtain the private key.

The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will delete the key after a time specified in the window. After that, nobody and never will be able to restore files...

To obtain the private key for the computer, which will automatically decrypt files, you need to pay 100 USD / 100 EUR / similar amount in another currency.

Click <close> to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.
Nuisances

• Chain Letters, petitions, etc.
  – Some have been circulating for years.
  – Most have incorrect information.
  – If tempted to believe them, check snopes.com
  – Even if true, please don’t forward to everyone in your address book!

• Pop-up Ads
  – Appear in web browser, quite annoying
  – Solution: install a browser plugin called Adblock Plus.

• Toolbars
  – Installed with apps – look before you click.
About 50,800,000 results (0.25 seconds)

**Dropbox Download - Free Download. Version for Windows**

Ad [dropbox.pc-file.com/](https://dropbox.pc-file.com/)

Download Drop box now!

**Download Dropbox for Windows**

https://www.dropbox.com/downloading

Downloading Dropbox... Your Dropbox download should automatically start within seconds. ... Once the download finishes, click Run to start installing Dropbox.

**Install Dropbox on your Windows PC**

https://www.dropbox.com/install

Download Dropbox for free. Join the 200 million users and 4 million businesses who already love Dropbox's file backup, sync and sharing solution.
you to easily manipulate files and subfolders in it like if they were locally stored. What is more, you can access your Dropbox on any computer (and as a plus, it is also available for smartphones), and share an specific subfolder with as many users as you want.

**You will be shown the following offers:**

When Delta is displayed, you can choose to change the configuration for your homepage, new tab and your browser’s search provider. You can also select if you want to apply these changes to Firefox, Internet Explorer or Chrome.

The Delta toolbar offers you utilities such as an online translator, games, etc.

Whitesmoke Toolbar, Iminent Toolbar.

Additional offers that you can check on this page will also be displayed.

These offers will be displayed depending on the user’s location as well as the configuration of his/her PC, considered normal to display 2-3 offers. You also have the chance to reject all the offers at the start and during the process. Check the uninstall instructions.

If you want to download the file from the author's website you can click here, but PC-File is not responsible as it can not test its content for virus, spyware or malware.
A Note on Privacy

• General rule: assume anything you post to a website, Facebook, etc. is public and permanent.
  – Privacy policies change constantly and are confusing (perhaps deliberately so).
  – Remember, anyone who can see your stuff can re-post it to anyone else, or to the whole world.

• Email is kind-of private if the connection is encrypted (e.g. Gmail) but remember anyone who gets the email can send it to anyone else.

• Use bcc not cc when sending an email to a group of people who don’t all know each other.
Google Picture Search for “Roy Blake”

Taken about 20 years ago by John Clark for the NC Technology web site. A search of the college website doesn’t find me, but Google does!
Social Media

• When using one service (e.g. Facebook) to log into another, a lot of info can be given to the second service.

• OK if you don’t mind, but:
  – Assume everything you have put on Facebook will be known to the other service.
  – Some will be given automatically, some only if you give permission. You guess which!
From Facebook’s Site

When you connect with a game, application or website - such as by going to a game, logging in to a website using your Facebook account, or adding an app to your timeline - we give the game, application, or website (sometimes referred to as just "applications" or "apps") your basic info (we sometimes call this your "public profile"), which includes your User ID and your public information. We also give them your friends' User IDs (also called your friend list) as part of your basic info.
Managing E-Mail

– Check your spam folder --- there may be good messages there.

– With Gmail and Hotmail you can report spam by moving it to spam folder and report good messages by moving them to inbox.
  • That will improve the spam detection in the future.

– With ISP email accounts, there is a disk quota which, once exceeded, causes incoming emails to “bounce”
  • Example: Cogeco: 100 MB.
  • Solution: set email client to delete messages from server. You store them on your computer.
  • Or use a webmail service like Gmail (15 GB quota).
“Mailbox Full” Error Message

Your message cannot be delivered to the following recipients:

Recipient address:
@ms02.int.cogeco.net:979761@lmtpcs-daemon

Original address: xxxxx@cogeco.ca

Reason: LMTP transmission failure has occurred
Diagnostic code: lmtp;550 4.2.2 Delivery failed: Over quota

Remote system:
dns;ms02.int.cogeco.net (TCP|192.168.201.174|65247|192.168.201.181|225)
“Reverse Identity Theft”

• When signing up for email, people sometimes ignore the message that an address is already taken.
• They think they have an email address that is actually someone else’s.
• Then they give that email address out, but someone else gets their email.
If your email address is [first initial]@[last name].

You gradually get to know lots of older people who have the same name pattern.

Yes, I know it would make sense if that were your email address, but it's not.

But how did you get my number?

Your phone bill.
Your account details

Account number: 237299680
Mobile number: 07917 332672
Contract start: 19-Feb-14
Minimum commitment end: 18-Feb-16
UK data: 500MB
Monthly line rental: £25.00

Manage account

We hope you're happy with your new plan. If there's anything you're not sure about, you can cancel within seven working days.

Get the most out of Vodafone
Your VODAFONE order is due for delivery on 29th January

Your VODAFONE order will be delivered on 29th January by DPD. Can you please ensure someone is available to sign for your delivery at:

Mr Roy Blake
Thornden School Winchester Roa
Chandler S Ford
Eastleigh
Hampshire
SO532DW
Your VODAFONE order is due for delivery on 4\textsuperscript{th} February

Your VODAFONE order will be delivered on 4\textsuperscript{th} February by DPD. Can you please ensure someone is available to sign for your delivery at:

Baginton  
Unipart Technology Logistics  
Unit 12  
Hamilton Way  
Bermuda Park  
Nuneaton  
CV107RL

If you’re not going to be in, it’s not a problem as you can change your delivery date or ask us to deliver to your neighbour by clicking below:

[Change my delivery]
GOOD MORNING DR. BLAKE
WE SAW NANCY ON MONDAY MEL FOUND NOTHING CONCLUSIVE BUT FELT IT WAS MUSCLE RELATED

nancy sylk
nancy sylk1

THANKS
MOIRA

Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.

2 Attachments
Summary

• Keep everything up to date.
• Use Antivirus.
• Backup – then backup the backups!
• Read everything and think before clicking.
• Nobody is going to give you a million dollars.
• Real jobs don’t require upfront payment and don’t pay $150/hour.
• Don’t let anyone you don’t know work on your computer, especially over the phone.
• And finally:
Useful Links

• Avast antivirus: http://www.avast.com/en-ca/index
• Dropbox: https://www.dropbox.com/
• Password Safe: http://passwordsafe.sourceforge.net/
• Canadian Anti-Fraud Centre: http://www.antifraudcentre-centreantifraude.ca/english/home.html
• Snopes: http://snopes.com/