Computer Vandalism, Fraud and Other Forms of Thievery
Don’t be a Victim

By Phil Goff
Branch 116

July 19, 2012

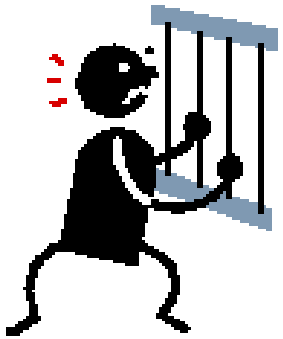
We're retired. Why would thieves bother with us?

- We have computers and use the internet
- We have credit cards with high limits
- We have bank accounts with substantial balances
- We aren't as quick thinking as we once were

We Are Prime Targets!

Don’t be Paranoid

- Computers are the best thing that has happened for Retirees since “senior discounts”
- Email, Digital Photos, Genealogy, Skype, etc is absolutely wonderful
- Be aware of the way thieves break in.
- Take simple precautions.
- Thieves will pick someone else.



It’s Easy to Defend Yourself. Just Be Aware!

Categories of Computer Fraud

Vandalism – No incentive to the perpetrator but to create mayhem

- Destructive Viruses, Malware, etc
- Emails warning you of “End of All Computing”
- Not much of a threat anymore
- Most Antivirus programs have blocked these efforts

Categories of Computer Fraud

Promises of Wealth – Classic emails telling how to get millions for free.

- Nigerian Scam (Spanish Prisoners scam from 1920's)
- Winning the Canadian or Irish Lottery
- Any other awards where you didn't enter the contest
- Don't fall for "Getting Something for Nothing."

Categories of Computer Fraud

<u>Convince You to Buy a Worthless Product</u> – Software, Phony Drugs, etc.

- Spam emails advertising products for sale
- Websites offering free computer scans to see if you need their antivirus product (you always do.)
- Telephone calls alerting you to computer problems.

Categories of Computer Fraud

Password Theft – Stealing passwords or other info to perpetrate fraud

- Thieves use your password to send emails to others
- If your credit card info is stored on a website, they may be able to log in and purchase goods.

Virus

A Virus is a computer program that can replicate itself and will do something bad

- Early ones were just mischievous. They didn't cause any real harm, may have moved an icon, etc.
- Really bad ones can cause irreparable harm to your data files
- May slow down your internet access, etc.
- Your best defense is smart computing and a good antivirus program

Spyware

Spyware tracks your computer activity and collects data on you.

- These are generally harmless and may actually make your computing more enjoyable.
- When you look at a product at a website like Amazon, a cookie (aka spyware) is placed on your computer.
- Advertisements on your computer will be targeted to your personal interests.
- You can clean out spyware with a number of free utility programs like Adaware, Spybot, Malware Bytes, etc.

Trojan Horse

A Trojan Horse is a virus that is disguised or hidden in other software.

- You may install a game or download free music that contains a Trojan Horse.
- A Trojan Horse program can do many bad things. It can be a keylogger, capture passwords and a lot more.
- Antivirus software will identify and block most Trojan Horses.

Malware

Malware (malicious software) is a generic term for software built to cause problems.

- Includes Viruses, Trojan Horses, Keyloggers, etc.
- Blocking and removing requires 3 Steps:
  - Intelligent computing
  - Good AntiVirus software
  - Running Malware removal programs periodically.

Worms

Worms are special viruses aimed at Servers

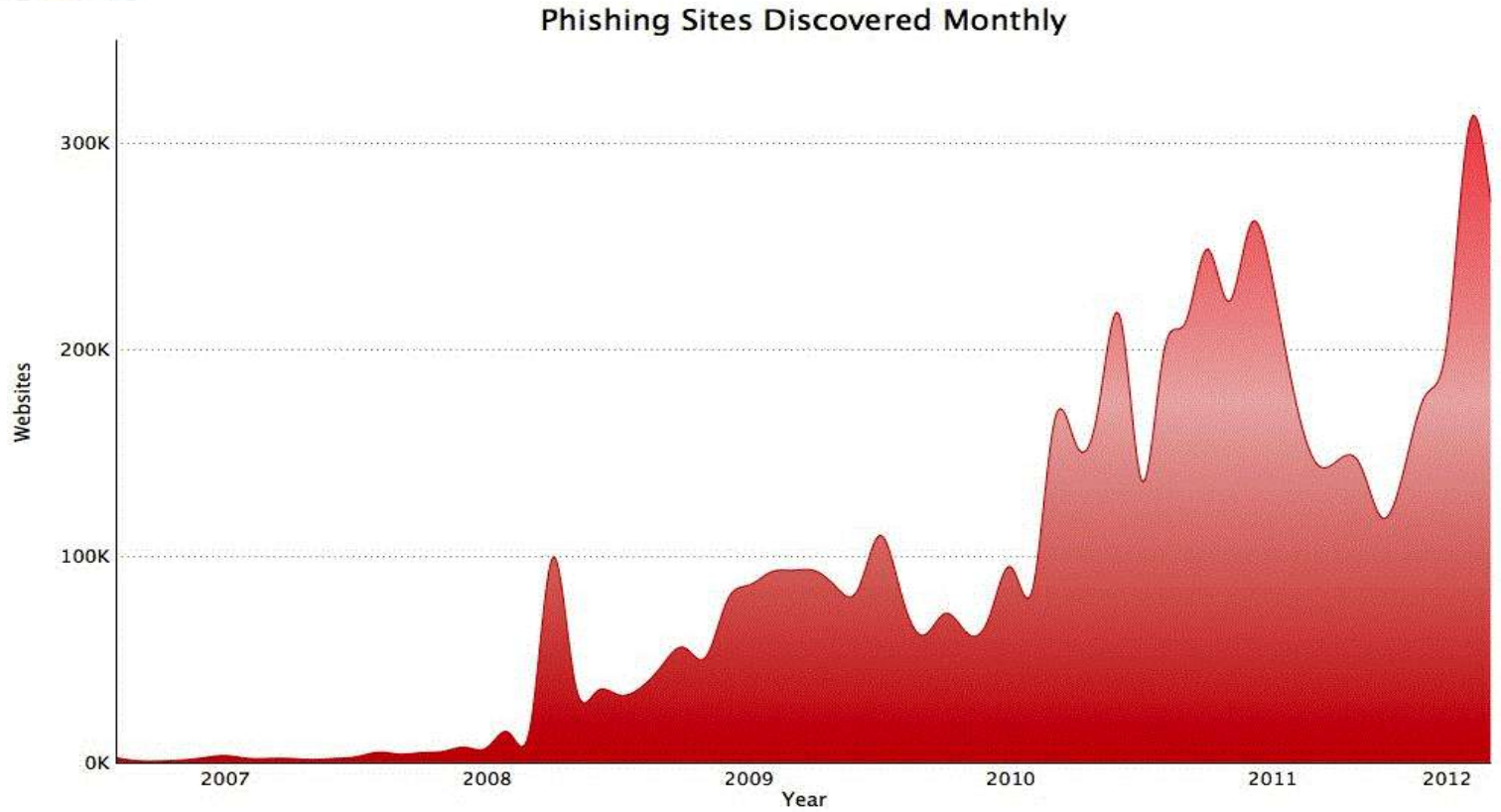
- If a worm is successfully inserted into a server, it can infect huge numbers of computers
- There isn't much we can do about worms. The companies who run servers watch for them.

Phishing

Phishing is insidious and dangerous

- Crooks create websites that look like a bank website or other legitimate business.
- The phony website asks you for sensitive information, e.g. your password, credit card number, etc.
- ***Never enter sensitive info into an email or link that was sent to you***. Always log into the true Company before changing passwords, etc.

Phishing



Google finds about 9500 new malicious websites each day

Spoofing

Spoofing means to send an email or make a telephone call that appears it is from someone else.

- Sending out emails that appear to be from someone they are not, i.e. phony name or organization.
- Hacking the telephone system so that Caller ID indicates a call is coming from a name and Area Code that is not theirs.

Pharming

Pharming is Relatively New

- Crooks create a Domain name that is spelled almost the same as a legitimate Company.
    - e.g. BankofAmerica.com is correct. They register a domain name of BankofAmarica.com.
    - If you happen to spell the Company name wrong, you are taken to the wrong website which will collect info from you.
- Big Companies watch for these sites and they are rarely successful.

How Do They Steal My Address Book?

They steal your password.

- When you register at some site with username and password, most people use the same password for email. Thieves may get that list.
- You unwittingly give thieves your email password.
- They have very fast computers that try every possible combination of letters and easily crack simple passwords.
- You click on a link in an email that was phony (e.g. email from UPS or DHL about a package for you)

How Do They Steal My Address Book?

They steal your password (cont.)

- Used a public computer or WiFi network
- Clicked on a link I received from a friend in Facebook

Phishing for Yahoo Passwords

YAHOO! MAIL Beta

Dear User,

Due to the congestion on our server, we regret to announce to you that all unused accounts will be shut down permanently.

You will have to confirm your Yahoo! Mail account. So you are required to logon to your Online Yahoo! Mail Account with the provided link below.

https://mail.yahoo.com/32131-111/aol-1/update/287329199200001290011/Suite.aspx
NB: Failure to to update your Yahoo! account will result to a permanent closure.

Thank you for being a loyal Yahoo! Mail user.

We hope you enjoy the newest version of Yahoo! Mail.

Phishing for Yahoo Passwords

Find a Home | Luxury Home Search | Comparable Home Sales

RE/MAX

Outstanding agents. Outstanding results.®

Dear Friend,
You might be interested in this special selected properties for June. Make 70% return on investment now.
To check these properties out, CLICK HERE. and log in with your email.
Respectfully,

Marlene M Talbot™, *Associate Broker*
Certified Residential Specialist
RE/MAX Realty Group

RE/MAX MISSION REALTY

SIR Members with Address Books Stolen

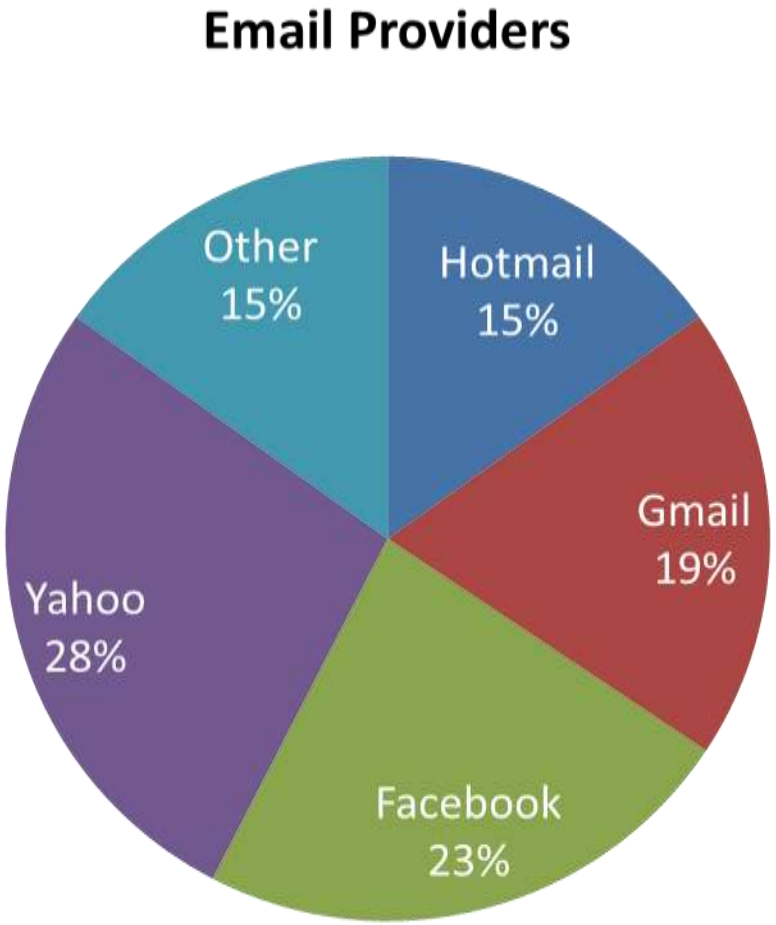
First	Last	ISP			
Richard	Ahlf	SBCGlobal			
Don	Degraf	Yahoo			
Tom	Eller	Yahoo			
Al	Foley	SBCGlobal			
Dudley	Hattaway	Comcast	Virus "Pup.funmoods"		
Bill	Hemmelsbach	SBCGlobal			
Pete	Kallas	SBCGlobal			
Dick	Kauffman	Yahoo			
Jim	Nachtweih	SBCGlobal			
Glen	Renk	Yahoo			
Ralph	Thornicroft	AOL	Suspects a Trojan Horse		
Tom	Whitten	pacbell			
Leary	Wong	Yahoo			

Why So Many Stolen Address Books

- In March 2011 the Rustock botnet was taken down by a Microsoft led consortium
  - Rustock was responsible for over 30% of global spam
  - New botnets can be taken down using IP reputation software

- Many Spammers changed from botnets to compromised email accounts
  - It’s hard to block compromised account emails since they are legitimate accounts
  - Spammers can establish their own accounts but Service Providers can spot them quickly.

Which Emails are Targeted?



Yahoo May Have Been Compromised

- Recent reports are that Yahoos email system has been hacked by some programmers in the Ukraine.
- If that is true, then expect to see more email spam from Yahoo users.

Telephone Scams

Crooks have been telephoning from outside of the Country. There is no way to stop them.

- Claim they are from Microsoft and there is a problem with your computer.
- Ask you to type something into your computer that will generate error messages and then sell you antivirus software
- Many other claims:
  - Grandson calling who needs money
  - You just won the lottery

How Do We Protect Ourselves?

1. **Always have an Antivirus program installed on your computer.**

    - Most are good enough for us.
    - If you have Comcast use their free Norton Antivirus program
    - Use one of the the top three free programs:
        - Microsoft Secuity Essentials
        - AVG
        - Avast

    - Make sure your AntiVirus software is up to date.

Note: Only run one AntiVirus program. More than one can corrupt your computer.

What are Best Free Security Programs?

Hint: Go to CNET Downloads and see which are the most popular. Browse to http://download.cnet.com

MOST POPULAR DOWNLOADS

DOWNLOADS FOR LAST WEEK

1.	AVG Anti-Virus Free Edition 2012	1,214,649
2.	Avast Free Antivirus	1,024,343
3.	CCleaner	461,606
4.	Malwarebytes Anti-Malware	427,246
5.	TeamViewer	341,608
6.	YTD YouTube Downloader & Converter	341,550
7.	Advanced SystemCare	311,232

How Do We Protect Ourselves?

2. Use Good Passwords

- Create 8 character passwords with at least 2 numbers in them
  - Don’t just put a “1” at the end

- As a minimum, use at least 3 separate passwords:
  - One for email
  - One for Banking or other financial
  - One for everything else.

- Use a password manager program or write them down.
  - There are several excellent password manager programs that are free
  - Create a simple Excel or Word file to record your passwords.

Password Manager Programs

Name	Price	Store on Computer or Server?	Security	Notes:
Roboform	$29.95*	Computer	Excellent	Passwords can be stored on USB flash drive.
1Password	$49.95	Computer	Excellent	Expensive but very slick.
LastPass	Free or $1/mo	Server	256bit	Free version has some advertising. Paid version has mobile access.
KeePass	Free	Computer	Uses key files	Older software.

*Licensed to one computer. Monthly fee allows access to all mobile devices.

How Do We Protect Ourselves?

3. Periodically run a Malware removal program.

- The most popular free utilities are:
  - Malware Bytes
  - Ccleaner
  - Spybot Search and Destroy
  - Adaware
- You can have more than one on your computer and run them as often as you wish. Once a month is probably sufficient.

How Do We Protect Ourselves?

4. Be Intelligent about your computing practices

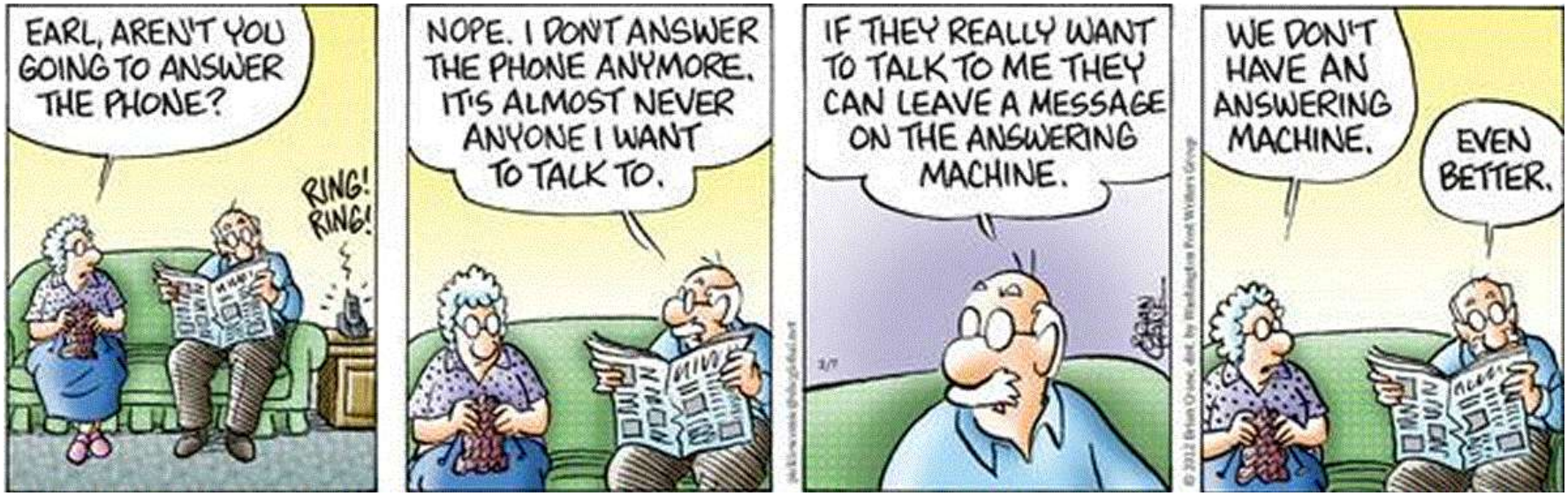
- Don’t open email attachments from people you don’t know
- Don’t enter your Userid or Password unless you are certain of the website’s authenticity
- Don’t download music, video or other stuff unless it is from a reputable site, e.g. iTunes, YouTube, Netflix, etc.
- If your antivirus program pops up a warning, read it carefully.

How Do We Protect Ourselves?

5. Don’t Fall for Telephone Scams

- Never give sensitive information to someone who calls you. Ask for their Company name and call that Company back.
- Microsoft or other computer people will never call you. They don’t know if you own a computer.
- If they say they are from the Credit Card fraud division, hang up and call the number on the back of your credit card.
- If they say they are your grandson, ask questions.
- Use Caller ID. If you don’t know the number that is calling, let it go to the answering machine.

How Do We Protect Ourselves?



Don’t Let the Bad Guys Ruin Your Fun

Computers and Internet are Wonderful

- They have become a part of our daily lives and are lots of fun
- There will always be bad guys, but it’s simple to get them to look elsewhere for “easier pickings”
- Be aware of the major fraud practices so that you can advise others. Many elderly people don’t understand and are easily defrauded.