

Scared Safe:

Life's Little Identity Theft Prevention Handbook

Todd M Feinman



identityfinder



Table of Contents

Foreword and Introduction	2
Peer-to-Peer File Sharing	6
Viruses and Worms	10
Bots and Trojans	14
Web Application Exploits	18
Spyware	22
Phishing	26
Smishing and Vishing	30
Receipts	34
USB Drives	38
Retiring a Computer	42
Identity Finder Software	46
Additional Resources	50



Foreword

Every day identity theft threatens you, your family, and your peace of mind. Preventing identity theft is a multi-step approach that requires awareness, changes in behavior, and security tools. Your identity is stored electronically much more frequently than you realize. It is critical that you take steps to protect that identity before it is too late.

Credit card numbers, social security numbers, passwords, bank accounts and other personal information are the constant targets of hackers and identity thieves.

This comprehensive, yet easy-to-understand guide explains some of the most common threats - and most importantly - how you can protect yourself from being their victim.



How Big is Identity Theft?

- According to the FTC over 9 million Americans' identities are stolen each year.
- Of all complaints received by the FTC in 2007, the highest category was related to identity theft encompassing 32%.
- Consumers reported fraud losses totaling more than \$1.2 billion in 2007. This is almost double of 2005.
- Over \$100 billion in identity theft has been reported by consumers and businesses over the past two years.
- Average fraud is estimated at \$500 out of pocket and 30 hours of time spent per victim to resolve the problem.
- 64% of fraud complaints where the company's method of initial contact was reported as Internet solicitations: electronic mail comprised 49% and web comprised 15%.



The Market for Identity Theft

- IDC estimates that the black market trafficking of stolen electronic identities will increase to \$1.6 billion in 2010.
- According to a 2007 US Department of Justice study on the illegal selling of stolen identities:
 - Stolen credit card information was sold for between \$0.50 and \$5.00 per card
 - Stolen bank account information was sold for between \$30.00 and \$400.00
 - Full identity information was sold for between \$10.00 to \$150.79
 - This stolen personal information is typically available on illegal underground Web sites.



Identity Theft Black Market Example

- Actual screenshot of an illegal website displaying stolen bank account logins. Thieves can view how much money is remaining in each account and purchase your login and password:

Bank Name	Country	Balance	Price
Bank of America (BOA)	USA	...	Sold
Amsouth Bank	USA	\$16,040	€700
Washington Mutual Bank(WAMU)	USA	\$14,400	€600
Washington Mutual Bank(WAMU)	USA, Multi-currency acct.	\$7,950 + £2,612	€500
Washington Mutual Bank(WAMU)	USA	...	Sold
MBNA America Bank	USA	\$22,003	€1,500
BANCO BRADESCO S.A.	BRAZIL, Dollar Account	\$13,451	€650
CITIBANK	UK, GBP Account	£10,044	€850

Source: http://news.cnet.com/8301-10784_3-9939862-7.html?tag=bl



Peer-to-Peer (P2P) File Sharing



identityfinder

Threat Information

- P2P File Sharing is a very common application used by children and adults to download music, videos, and games.
 - The SANS Institute has identified file sharing applications as one of the most crucial internet security vulnerabilities.
 - Kids & Digital Content reports that 70% of kids ages 9 through 14 are downloading digital music and The NPD Group has stated, "high levels of illegal peer-to-peer (P2P) file sharing" are attributed as the source of those downloads.
- Recently a 35 year old Seattle man plead guilty to using peer-to-peer file-sharing programs such as Limeware to steal personal information from tax returns, credit reports, bank statements and student financial aid applications.
 - http://www.upi.com/NewsTrack/Top_News/2007/11/05/seattle_man_guilty_in_id_theft_case/2352/



Tax Return File Sharing Example

- Tax returns are rife with personal information and easily accessible to the public over P2P File Sharing:

The screenshot shows the LimeWire interface with search results for tax returns. The search filters are set to ".tax (3)" and "tax return (416)". The results table lists various tax return files, including "2007 Vitania's Tax Return", "2005 joanna_jankulski_Return", "2005 tax return", "2006 Barbara's Tax Return", "2005_Federal_Return", "2005 tax return malissa", "2004 James's Tax Return", "2006 James's Tax Return", "2005 James's Tax Return", "John Wiley & Sons, Make Money in Real Estate ...", and "Fixed Asset Changes for the Tax Return".

Quality	#	Lice...	Name	T...	Size	Speed	Bitrate
★★★★★			2007 Vitania's Tax Return	pdf	196.9 KB	Broadband	
★★★★★			2005 joanna_jankulski_Return	pdf	22.0 KB	T3 or Hi...	
★★★★★			2005 tax return	pdf	249.8 KB	T3 or Hi...	
★★★★★			2006 Barbara's Tax Return	pdf	39.0 KB	T3 or Hi...	
★★★★★			2005_Federal_Return	pdf	11.2 KB	T3 or Hi...	
★★★★★			2005 tax return malissa	pdf	12.1 KB	Broadband	
★★★★★			2004 James's Tax Return	pdf	107.0 KB	T1	
★★★★★			2006 James's Tax Return	pdf	151.1 KB	T1	
★★★★★			2005 James's Tax Return	pdf	103.7 KB	T1	
★★★★★			John Wiley & Sons, Make Money in Real Estate ...	pdf	2,404 KB	T3 or Hi...	
★★★★★			Fixed Asset Changes for the Tax Return	QBR	10.0 KB	Dial Up	

Example of a quick, simple, search on common file sharing network for tax returns.

How to Protect Yourself

- Never share personal folders.
- Shred any files containing personal information you do not need and secure (encrypt) any files you do need so that if inadvertently exposed, you are not at risk.
- Turn off file sharing when not in use.
- Always upgrade to latest version.
- Do not download illegal files as they could contain malicious code.



Viruses and Worms



identityfinder

Threat Information

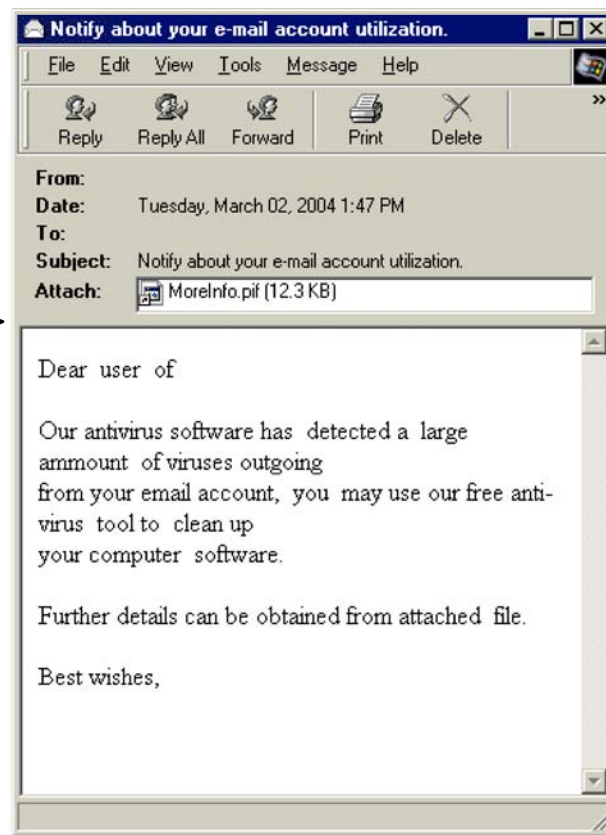
- Viruses and Worms are malicious programs written with the intent to harm your computer.
- In some cases, the worms spread by emailing files to other people – files that could potentially contain confidential information!
- New strains are released every day making them difficult to avoid.



Worm Example

- The Bagle worm infected users' systems via an e-mail attachment and then mass re-emailed itself to others. There were 60-100 variants and many opened a back door on the infected PC that allowed thieves to access personal and financial data.

Example of an email that re-mails itself to people in your contacts folder.



How to Protect Yourself

- Do not store important passwords in your web browsers.
- Enable virus protection.
- Update your virus definitions daily or weekly.
- Shred any files containing personal information you do not need and secure (encrypt) any files you do need so that if ever emailed unbeknownst to you, they do not put your identity at risk.



Bots and Trojans



identityfinder

Threat Information

- Bots, Trojans, and other malware can open backdoors that enable attackers to control a computer and steal confidential information. According to Microsoft Trojans and Bots are a significant and tangible threat to Windows users.
- Microsoft's malware removal tool has removed at least one backdoor Trojan from approximately 3.5 million unique computers or 62% of users running the application.
 - <http://www.microsoft.com/downloads/details.aspx?FamilyId=47DDCFA9-645D-4495-9EDA-92CDE33E99A9&displaylang=en>



Botnet Example

- A 26 year old wrote computer code known as a botnet to attack computers unbeknownst to the users while they performed all their daily activities. However, the botnets were collecting personal information from their computers and sending it to the hackers. The hackers then used that personal information to log into the victims' paypal accounts and steal money. The hacker admitted to infecting 250,000 PCs.

- <http://www.latimes.com/business/la-fi-botnet10nov10,1,3400959.story?coll=la-headlines-business>

Bots can read stored passwords from your web browsers...

Account login

Email address
joe@google.com

PayPal password
.....

Log In

Forgot your [email address](#) or [password](#)?

New to PayPal? [Sign up](#).

How to Protect Yourself

- Enable malware protection.
- Run Microsoft's free Malicious Software Removal Tool.
- Use personal firewalls and block unnecessary traffic.
- Do not store saved passwords for very important websites like you bank account.
- Periodically review what passwords are stored by your web browser.
- If possible, use a master password to encrypt all stored web browser passwords.
- Shred any files containing personal information you do not need and secure (encrypt) any files you do need so that if stolen, you are not at risk.



Web Application Exploits



identityfinder

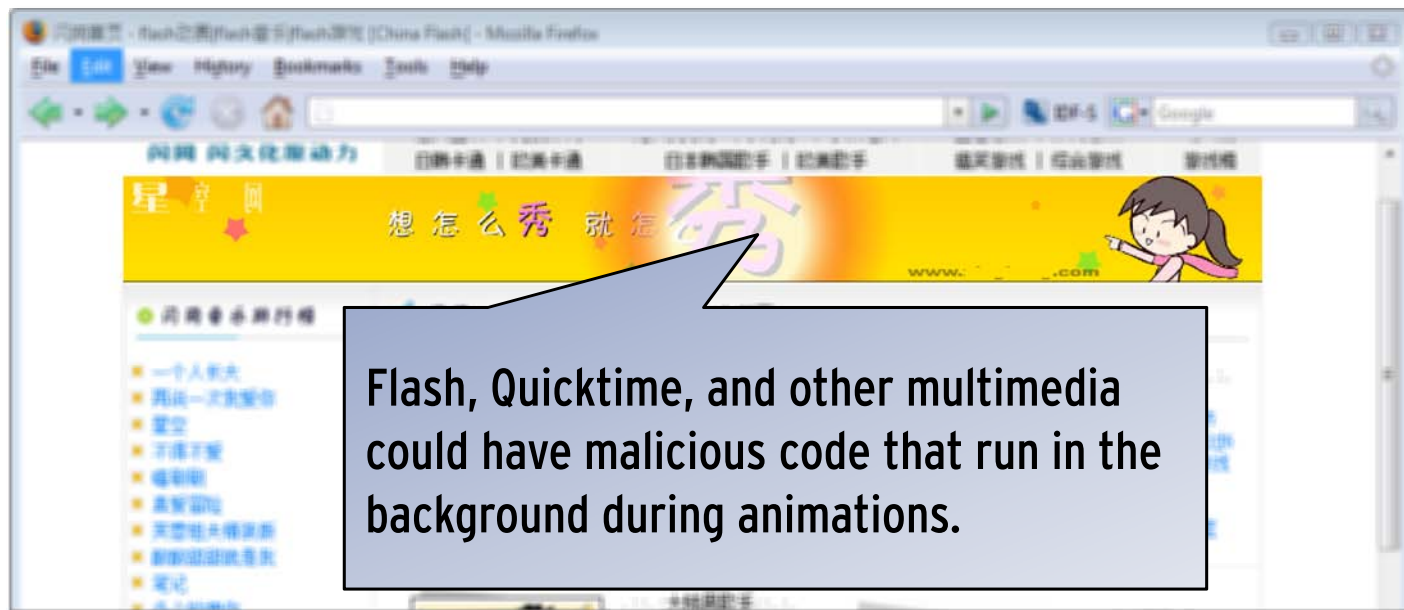
Threat Information

- Increasingly sophisticated website attacks that exploit browser vulnerabilities, especially on trusted websites, are listed as #1 in the top ten cyber security menaces for 2008 by San Institute.
 - Source:www.sans.org/2008menaces/?utm_source=web-sans&utm_medium=text-ad&utm_content=text-link_2008menaces_homepage&utm_campaign=Top_10_Cyber_Security_Menaces_-_2008&ref=22218
- Web site attacks on browsers are increasingly targeting rich media commonly viewed by web surfers (such as Flash and QuickTime). Most people don't update their web browser or these components often.
- These flaws have been widely exploited to install spyware, adware and other malware on users' systems.



Web Application Exploits

- Websites may have malicious code that steal your identity. Users are sometimes misdirected to these sites.
- One of the latest such modules, MPack, produces a claimed 10-25% success rate in exploiting browsers that visit sites infected with the module.



How to Protect Yourself

- Do not visit untrusted websites.
- Enable popup blockers to prevent any sites from misdirecting you to other untrusted sites.
- Update your multimedia players (i.e., Adobe Flash, Apple Quicktime, Microsoft Silverlight, etc.) monthly.
- Shred any files containing personal information you do not need and secure (encrypt) any files you do need so that if stolen, you are not at risk.



Spyware



identityfinder

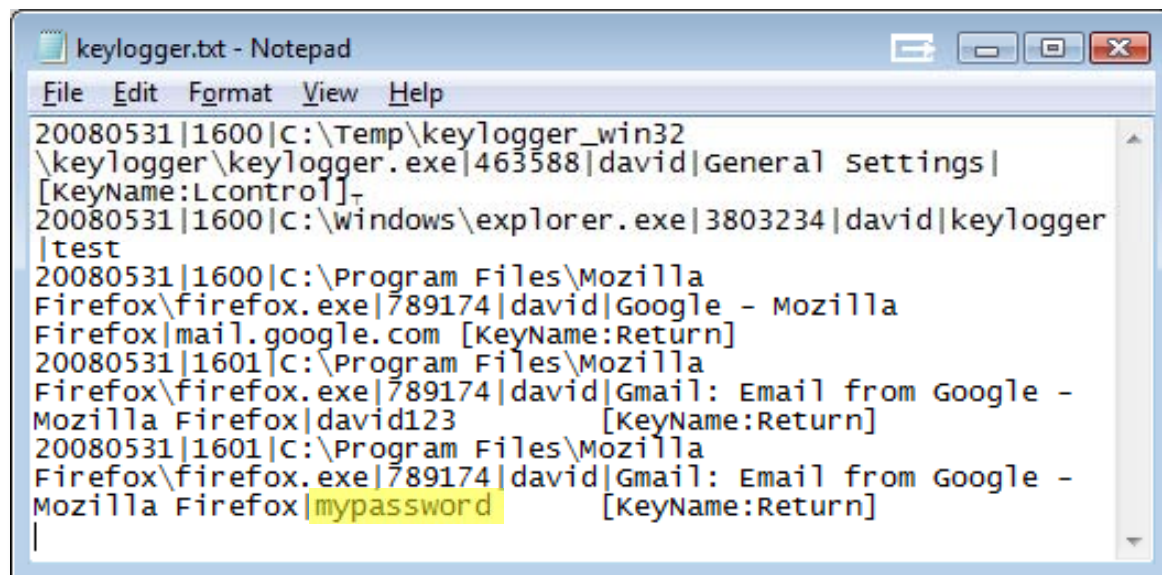
Threat Information

- Spyware programs are often installed behind the scenes in combination with a “free download” and runs without you knowing.
- Some spyware can record keystrokes (known as keyloggers) and send them to a server for hackers to view.
- When you log into a website and type a username and password, this is sent to a hacker’s server.
- Hackers then take this information, visit the same websites you did, such as your bank, and then log in as you and withdraw funds.



Keylogger Example

- Disguised as a program you think should be running, the keylogger records every keystroke and sends your personal information across the internet.



```
keylogger.txt - Notepad
File Edit Format View Help
20080531|1600|C:\Temp\keylogger_win32
\keylogger\keylogger.exe|463588|david|General settings|
[KeyName:Lcontrol]-
20080531|1600|C:\windows\explorer.exe|3803234|david|keylogger
|test
20080531|1600|C:\Program Files\Mozilla
Firefox\firefox.exe|789174|david|Google - Mozilla
Firefox|mail.google.com [KeyName:Return]
20080531|1601|C:\Program Files\Mozilla
Firefox\firefox.exe|789174|david|Gmail: Email from Google -
Mozilla Firefox|david123 [KeyName:Return]
20080531|1601|C:\Program Files\Mozilla
Firefox\firefox.exe|789174|david|Gmail: Email from Google -
Mozilla Firefox|mypassword [KeyName:Return]
```

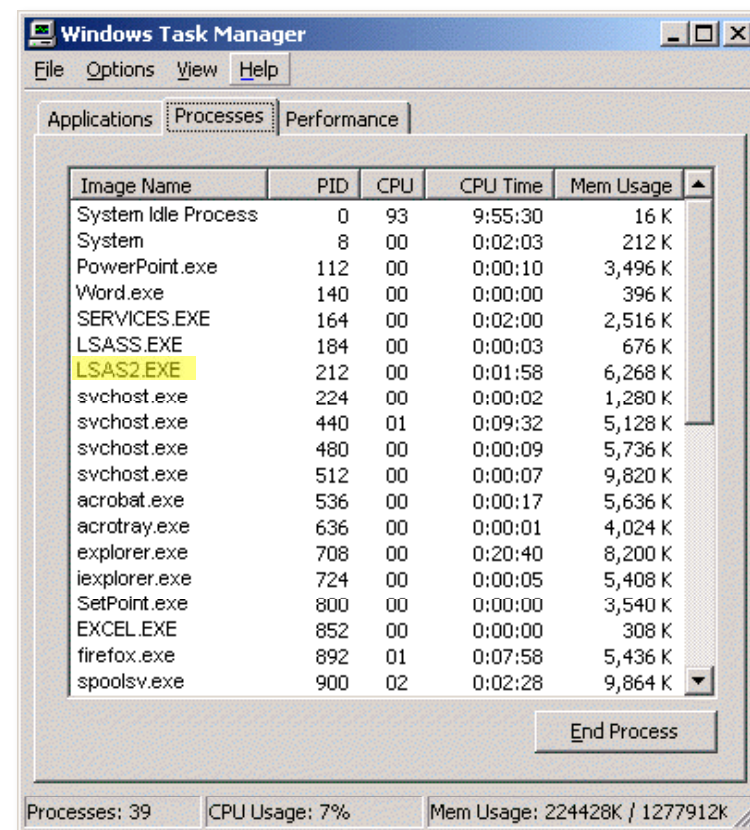


Image Name	PID	CPU	CPU Time	Mem Usage
System Idle Process	0	93	9:55:30	16 K
System	8	00	0:02:03	212 K
PowerPoint.exe	112	00	0:00:10	3,496 K
Word.exe	140	00	0:00:00	396 K
SERVICES.EXE	164	00	0:02:00	2,516 K
LSASS.EXE	184	00	0:00:03	676 K
LSAS2.EXE	212	00	0:01:58	6,268 K
svchost.exe	224	00	0:00:02	1,280 K
svchost.exe	440	01	0:09:32	5,128 K
svchost.exe	480	00	0:00:09	5,736 K
svchost.exe	512	00	0:00:07	9,820 K
acrobat.exe	536	00	0:00:17	5,636 K
acrotray.exe	636	00	0:00:01	4,024 K
explorer.exe	708	00	0:20:40	8,200 K
ieplorer.exe	724	00	0:00:05	5,408 K
SetPoint.exe	800	00	0:00:00	3,540 K
EXCEL.EXE	852	00	0:00:00	308 K
firefox.exe	892	01	0:07:58	5,436 K
spoolsv.exe	900	02	0:02:28	9,864 K

How to Protect Yourself

- Enable spyware protection (i.e, Windows Defender).
- Update your definitions daily or weekly.
- Periodically review the programs in your Task Manager (or process list) and get familiar with what should and should not be listed there.
- Shred any files containing personal information you do not need and secure (encrypt) any files you do need so that if your computer is compromised, your most sensitive information is safe.



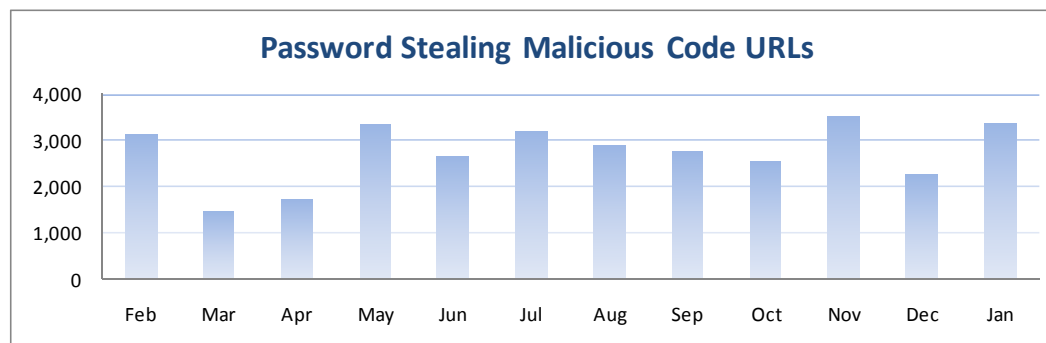
Phishing



identityfinder

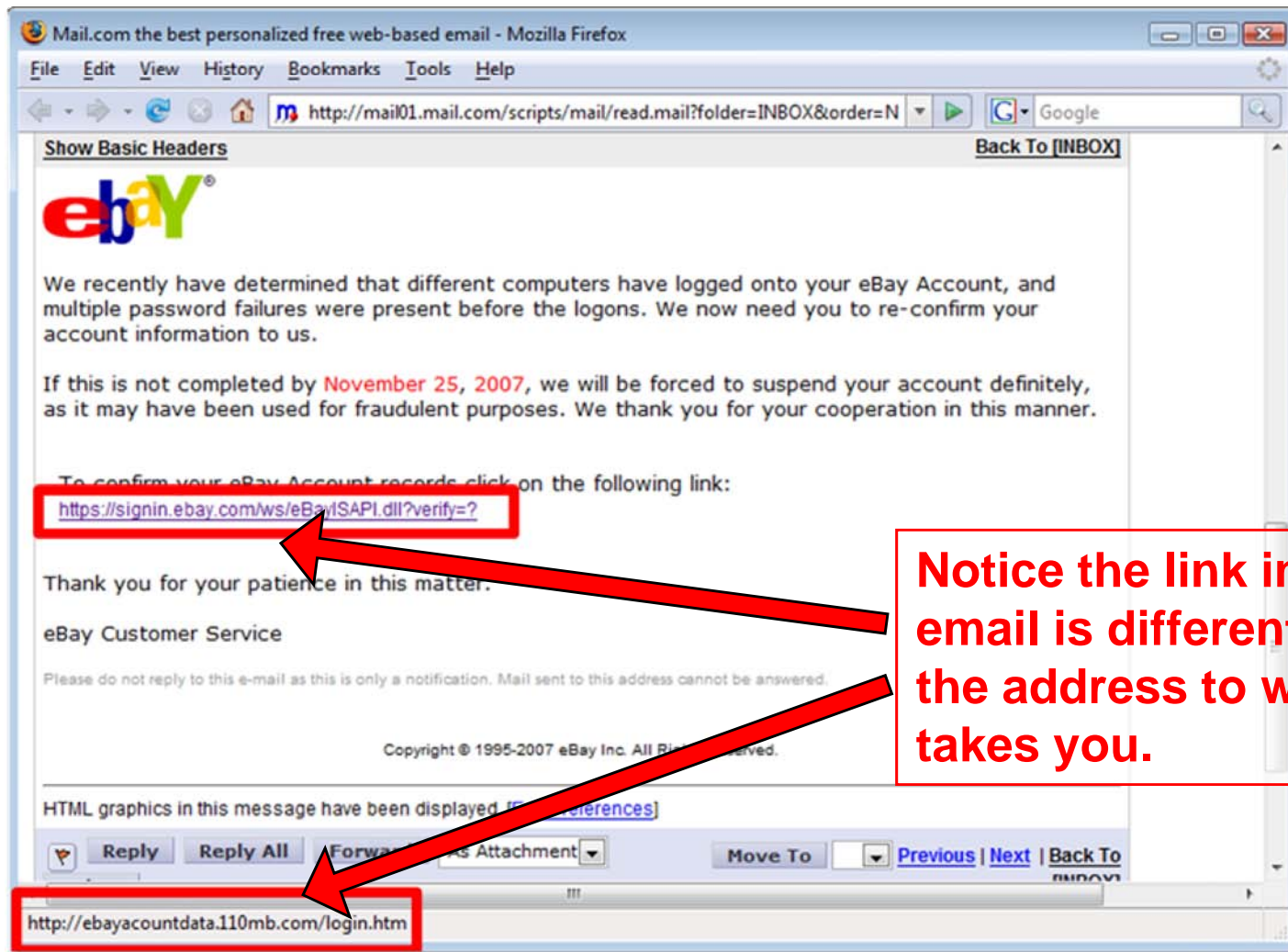
Threat Information

- Phishing is a common way to steal personal information by tricking the individual into entering their personal information into a website that is not what it appears to be.
- You might receive an email asking you to click a link to log into your eBay account, but the link really takes you to a thief's fake site which looks real and convinces you enter your password.
- According to the Anti-Phishing Working Group, over 32,000 password stealing URLs were reported in the twelve months ending Jan 2008.



Fake eBay Email Example

- Never click on links in emails because they can take you to different addresses than they display in the email:



How to Protect Yourself

- Never click on links in email messages - type them manually in your web browser.
- Enable junk mail (anti-spam) filtering to remove the majority of phishing attempts.
- Upgrade to the latest web browsers with phishing protection.
- Do not enter personal information on sites without the security Padlock (i.e., SSL).
- Make sure any website you visit displays the correct domain name (i.e., www.amazon.com).



Smishing and Vishing



identityfinder

Threat Information

- Smishing is SMS (text message) phishing or social engineering on your mobile phone. Vishing is voice phishing.
- For years, identity thieves have been calling people pretending to be from their bank, telling them that there is something wrong with their credit card, and asking them to provide some personal information so they can fix it.
- Today, this attack is commonly sent over to their phone as a text message.
- Victims click the link in the text message and call the number or go to a website.



Irregular CC Charge Example

From: 692639

Message: Irregular charge detected on your credit card account ending in 04321. Please call 1-800-XXX-9289.



How to Protect Yourself

- Always call the phone number on the back of your credit card or on your statement when you want to speak with your bank.
- Never give anyone your personal information (SSN or Credit Card Number) unless you trust them and they absolutely require it.
- Most businesses have no right to obtain your SSN. The Department of Motor Vehicles (DMV), Tax departments, and Welfare departments do require it. Any institutions performing tax transactions will also need it, such as banks, brokerages, and employers.
- Avoid giving it to other businesses. If they demand it, ask to speak to a manager, threaten to complain, and to see a written document stating they require it, and suggest alternative methods.



Receipts



identityfinder

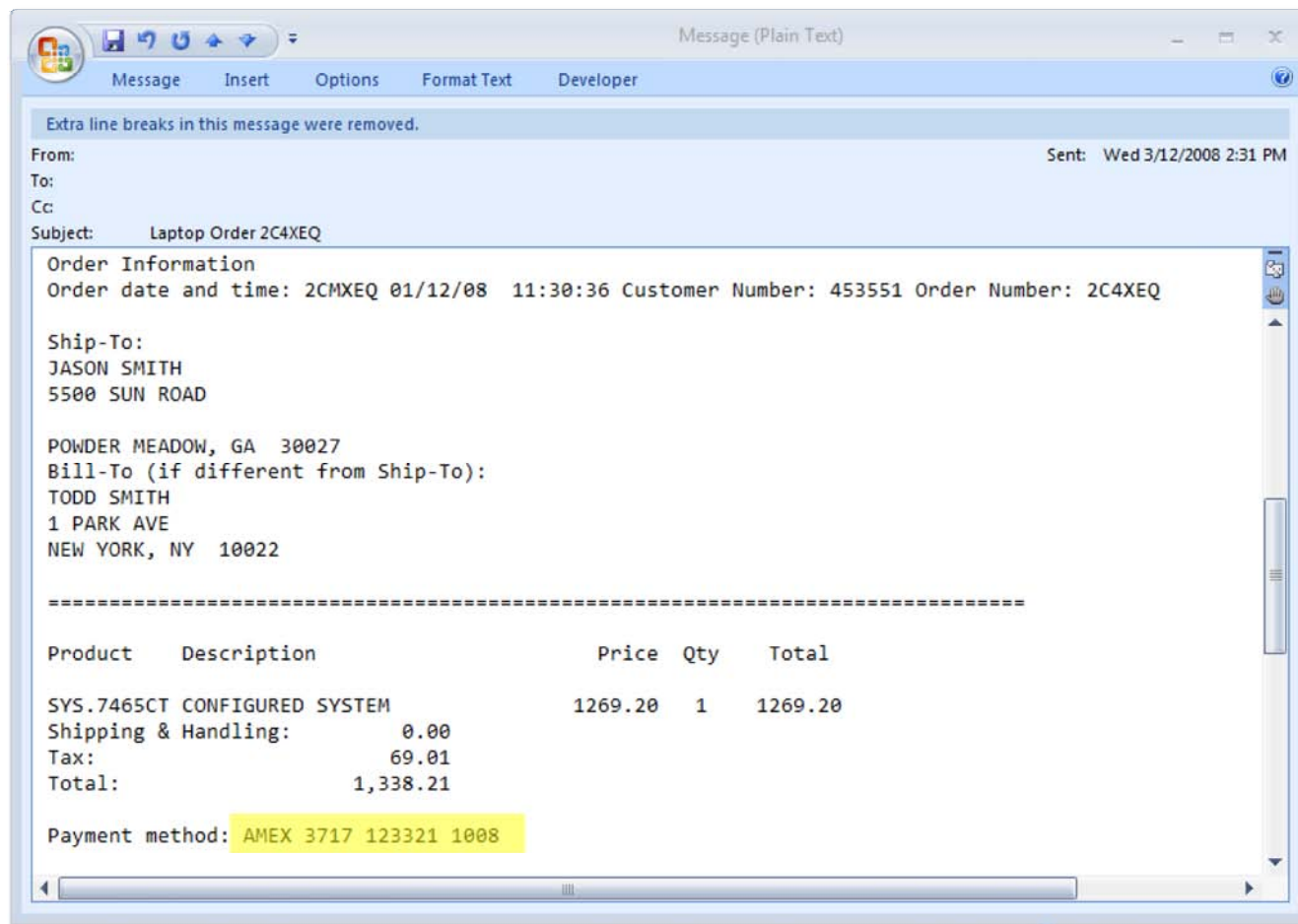
Threat Information

- After you make a purchase online you will typically see several forms of your receipt. Many retailers still record your entire Credit Card number in that receipt so you can verify it is correct.
 - The web page that displays your receipt is saved in your Temporary Internet Files cache.
 - Many people print that web page to a PDF for their records.
 - The retailer will also email you a copy of the receipt.



Emailed Receipt Example

- Many retailers still print your entire credit card number on receipts:



How to Protect Yourself

- Blackout your credit card number before scanning or printing to PDF.
- Shred any emails with receipts that you do not need.
- Redact credit card numbers from receipts that you do need.



USB Drives



identityfinder

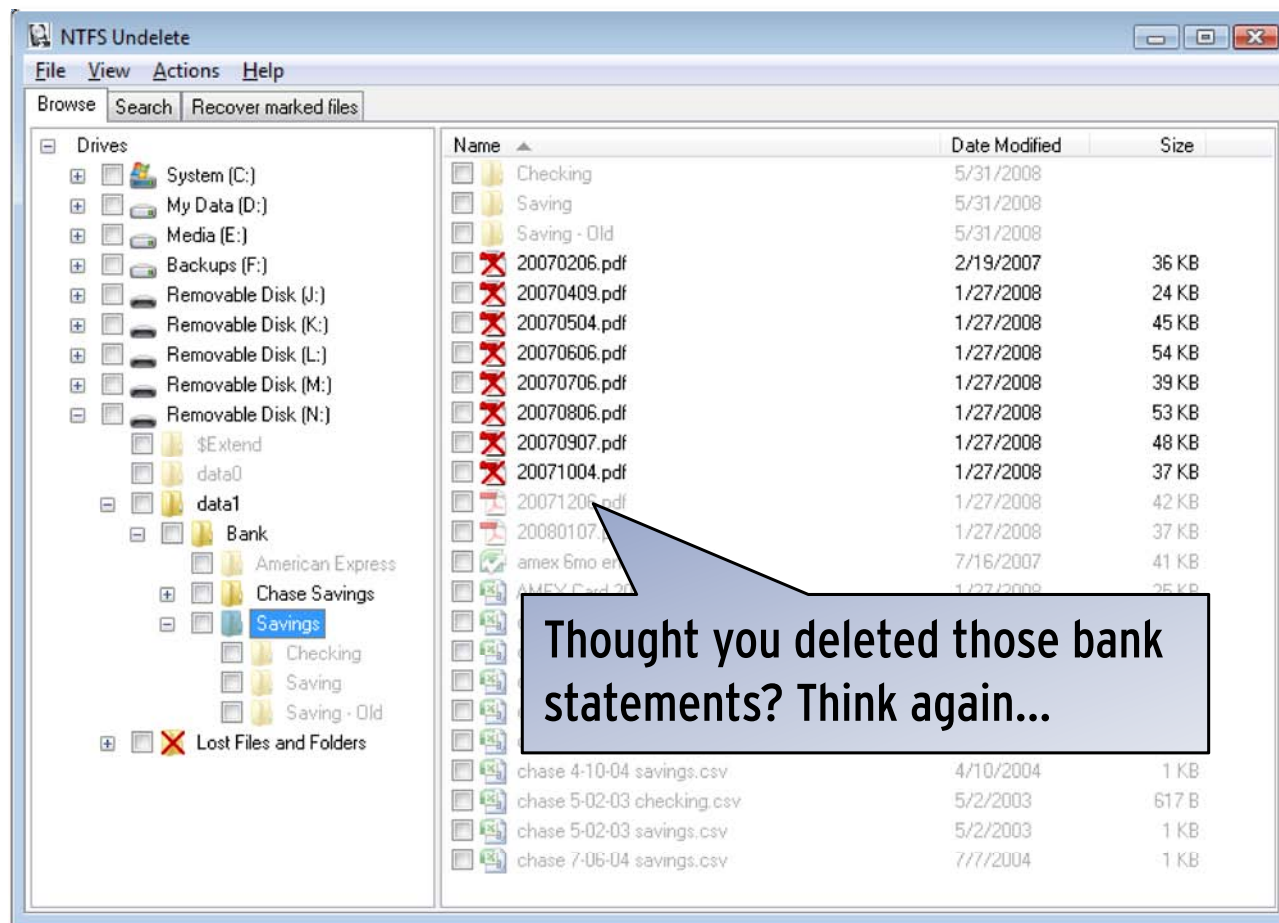
Threat Information

- People frequently swap or share USB flash drives with friends and colleagues. These flash drives sometimes have a lot of storage space but the files may only take up a small portion of that space.
- When files are deleted, they are easily undeleted, especially when there is a lot of free space on the drive. It is critical to always permanently shred any files with personal information.
- Digital shredders are not usually already on your computer so you need to download or purchase one. Emptying your recycle bin is not enough.



Undelete Example

- Deleted files are not truly deleted and can be easily undeleted with free programs:



How to Protect Yourself

- Do not leave your USB drives unattended.
- Do not lend your USB drives to people you do not trust unless you have shredded all files with personal information.
- Encrypt any files with personal information that you leave on the USB drive.

Retiring a Computer



identityfinder

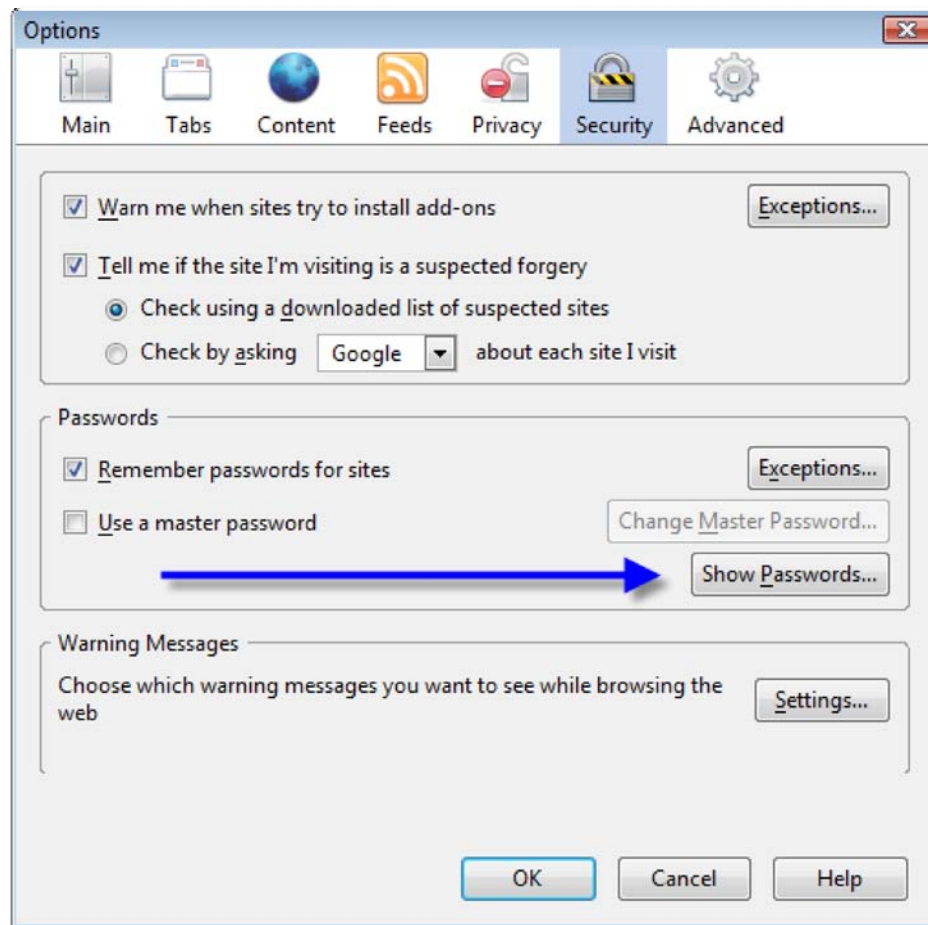
Threat Information

- When you retire or dispose of a computer, much of your information could be tucked away into hidden system areas you never knew existed. Simply deleting all your files is not enough.
- There are tons of personal information on computers' hidden areas. Credit cards, social security numbers, and passwords can be located inside your web browsers, IM chat logs, and Windows registry.



Selling/Donating a Computer Example

- There are many places on your computer (depicted by a web browser setting below) you do not realize your personal information is stored unprotected:



This web browser would let the next owner of your computer view the sites you visit and your passwords, if you didn't protect them.

How to Protect Yourself

- Shred all files with personal information.
- Format any hard drives used for data before disposing of or retiring your computer.
- If you plan to leave the operating system (such as Windows) in tact when handing down your computer, make sure you delete all your profiles as much personal information can be stored in the Windows Registry and other system areas.



Identity Finder Software

Preventing Identity Theft



identityfinder

Identity Finder

- Identity Finder helps you prevent identity theft by finding and protecting your personal information before it's too late.
- Identity thieves are always devising new ways to steal your information and even with dozens of security controls to stop them, sometimes they get through. When they do, you don't want them getting your identity.
- Identity Finder automatically finds Social Security Numbers, Credit Cards, Dates of Birth, Passwords, and Bank Accounts across your files, e-mails, and web browsers.
- Once found, Identity Finder helps shred the data you don't need and encrypt the data you do.





Start Stop

Search



Collapse All Rows Previous Match Next Match Filter Results

Review



Secure Shred Recycle Quarantine Open Ignore

Actions



Wizard

- Preview Pane
- Status Window
- Mask Passwords

View

<input checked="" type="checkbox"/> Location	Identity Match	#
<input type="checkbox"/> Internet Explorer Passwo...://www.velosecure.com/secure/form.pl	MyPassword01	1
<input type="checkbox"/> Internet Explorer AutoComplete: ssn	001-55-1234	1
<input type="checkbox"/> Firefox Password: https://www.identityfinder.com	MyPassword02	1
<input type="checkbox"/> Outlook: Inbox\support@velosecure.com\Login Info <Sa...:23 PM>	MyPassword03	1
<input type="checkbox"/> Outlook: Inbox\Doctor Smith\Health Record <Sun 2/11/...:28 AM>	001-55-1234	1
<input type="checkbox"/> c:\demo\bank statements\december 2006.pdf	9283-7476-5	7
<input type="checkbox"/> c:\demo\online receipts\amazon.html	4408-0412-5436-9873	2
<input type="checkbox"/> c:\demo\online receipts\identityfinder.html	54240000000000015	1
<input type="checkbox"/> c:\demo\online receipts\paypal.html	Multiple Matches	2
	3782 822463 10005	1
	6011 0009 9013 9424	1
<input type="checkbox"/> c:\demo\personal\cars.pptx	000-123-000	1
<input type="checkbox"/> c:\demo\personal\insurance.docx	Multiple Matches	4
	(212) 555-1234	1
	10 Park Ave, New York, NY ...	1
	January 1, 1970	1
	Smith	1
<input type="checkbox"/> c:\demo\personal\itinerary.doc	918273645	1
<input type="checkbox"/> c:\demo\sept archives\backup.zip <ftp.log>	MyPassword04	1

From: support@velosecure.com
Subject: Login Info
Date: Sat 1/20/2007 4:23 PM
Identity Type: 1 Password

Dear Alice Smith,

Thank you for signing up for Identity Finder development community!
 You may login and activate your account by visting:
<http://www.identityfinder.com/>
 Login: alicsmith
 Password: **MyPassword03**

Thank you for your business and we look forward to working with you!

Best regards,
 Velosecure Support Team
 Velosecure, LLC
 support@velosecure.com
<http://www.velosecure.com>
<http://www.identityfinder.com>

How to Protect Yourself

Three quick & easy steps to protecting you identity:

1. Download and install Identity Finder.
2. Let the Wizard search your computer's files, emails, and system areas. It will find personal information without you entering anything.
3. Review the results and safeguard your personal information:
 - Shred files you don't need.
 - Encrypt files that you do need.



Additional Resources

- Download Identity Finder Free Trial and Get Tips
 - www.identityfinder.com
- FTC's Identity Theft Site
 - www.consumer.gov/idtheft
- Identity Theft Resource Center
 - www.idtheftcenter.org
- Free Annual Credit Report
 - www.annualcreditreport.com
- Internet Crime Complaint Center
 - www.ic3.gov
- Consumer's Union
 - www.financialprivacynow.org
- Place a security freeze on your credit file:
 - www.consumersunion.org/campaigns/learn_more/003484individ.html



Copyright Identity Finder, LLC 2008.

This work is the intellectual property of the author. Permission is granted for this material to be shared for non-commercial, educational purposes, provided that this copyright statement appears on the reproduced materials and notice is given that the copying is by permission of the author. To disseminate otherwise or to republish requires written permission from the author.



identityfinder