Art Society of Monmouth County Presentation on 10/21/20

Cyber Security Program by Susan VanVolkenburgh

- In the past cyber security was a good virus program and a firewall.

ASMC

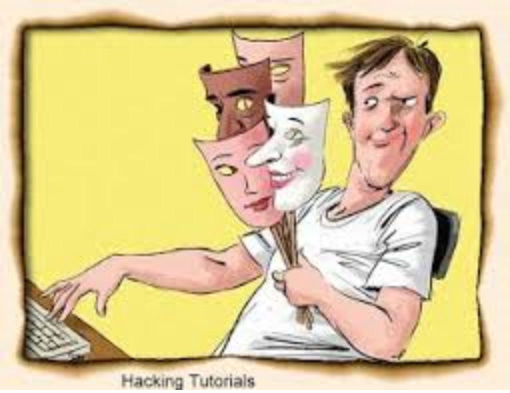
- Today cyber security is anti-virus programs, firewalls and vigilance on the part of every user.

DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
©2006 JOHN KLOSSNER, WWW.JKLOSSNER.COM

ASMC

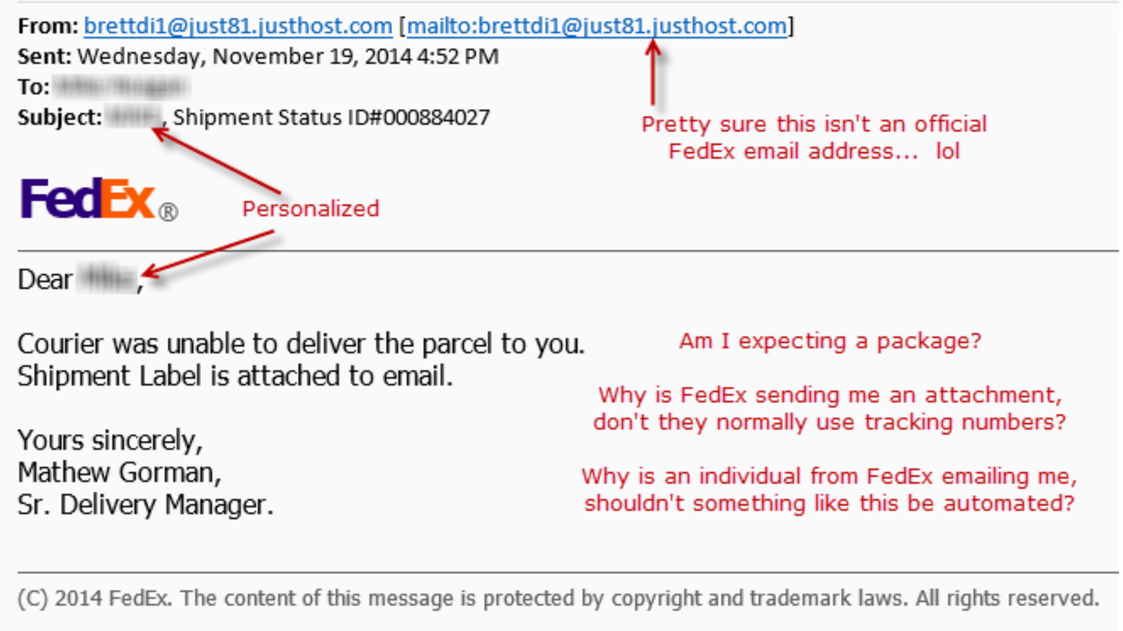
- Our program will show you how you are the front line of your defense and will help you to arm yourself against all invasions!

- Email – Who can I trust?
  - No one! Not a business colleague, not a contact in another company not even a friend or family.



- Email - What can I trust?
  - Nothing. Particularly attachments and links.

- How can I check email?
  - Check the mailto in From:.



From: brettdi1@just81.justhost.com [mailto:brettdi1@just81.justhost.com]
Sent: Wednesday, November 19, 2014 4:52 PM
To: [redacted]
Subject: [redacted], Shipment Status ID#000884027

FedEx®

Dear [redacted],

Courier was unable to deliver the parcel to you.
Shipment Label is attached to email.

Yours sincerely,
Mathew Gorman,
Sr. Delivery Manager.

(C) 2014 FedEx. The content of this message is protected by copyright and trademark laws. All rights reserved.

Pretty sure this isn't an official FedEx email address... lol

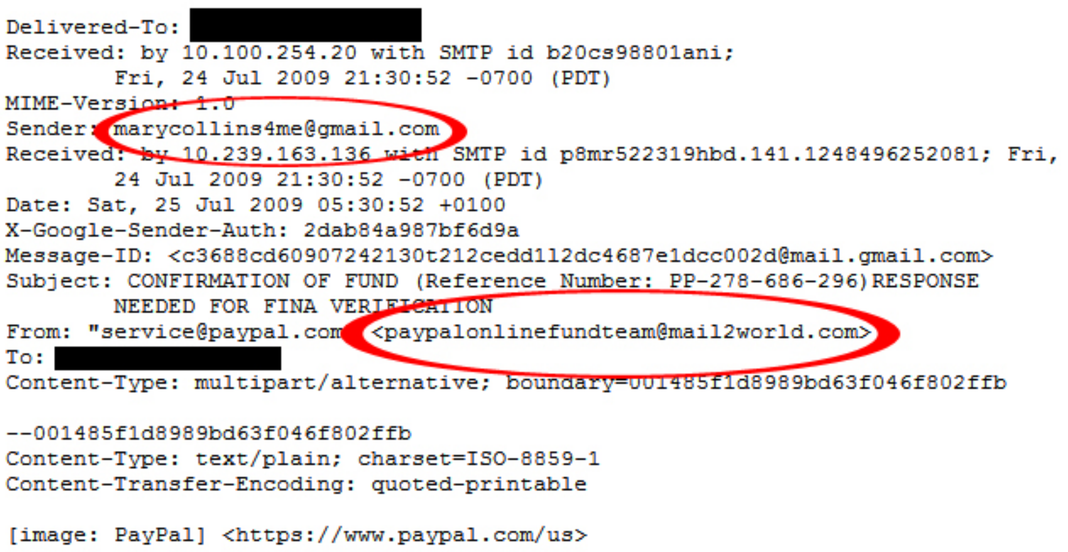
Personalized

Am I expecting a package?

Why is FedEx sending me an attachment, don't they normally use tracking numbers?

Why is an individual from FedEx emailing me, shouldn't something like this be automated?

- How can I check email? Cont’d
  - Check the mailto or send-to in header:.

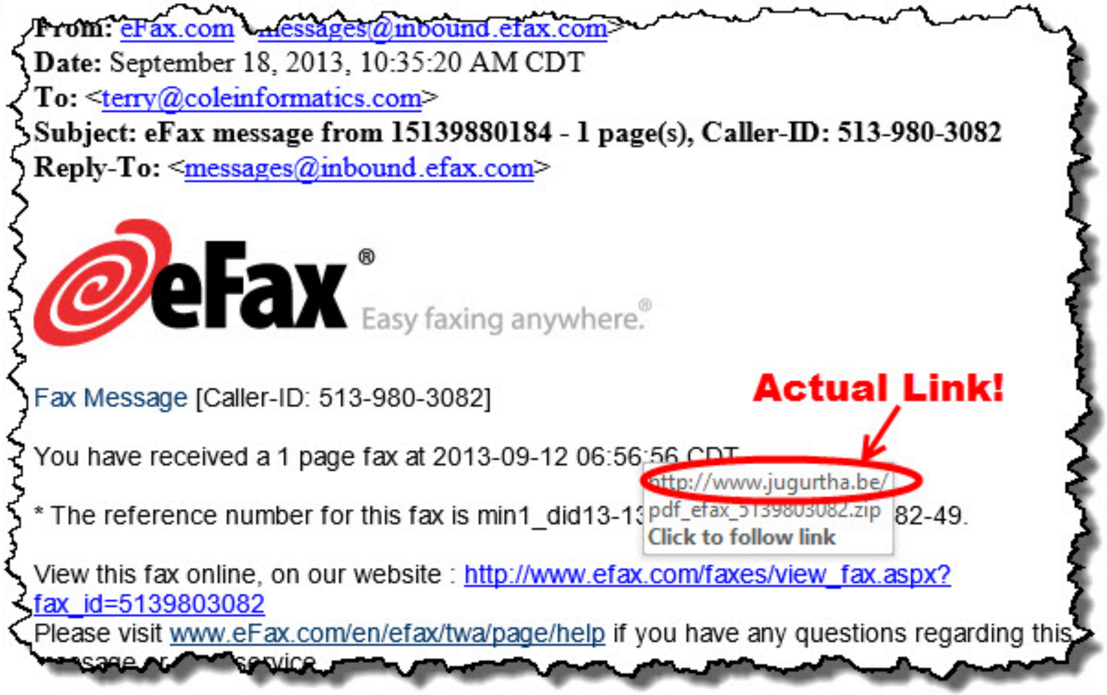


```
Delivered-To: [redacted]
Received: by 10.100.254.20 with SMTP id b20cs98801ani;
        Fri, 24 Jul 2009 21:30:52 -0700 (PDT)
MIME-Version: 1.0
Sender: marycollins4me@gmail.com
Received: by 10.239.163.136 with SMTP id p8mr522319hbd.141.1248496252081; Fri,
        24 Jul 2009 21:30:52 -0700 (PDT)
Date: Sat, 25 Jul 2009 05:30:52 +0100
X-Google-Sender-Auth: 2dab84a987bf6d9a
Message-ID: <c3688cd60907242130t212cedd112dc4687e1dcc002d@mail.gmail.com>
Subject: CONFIRMATION OF FUND (Reference Number: PP-278-686-296)RESPONSE
        NEEDED FOR FINA VERIFICATION
From: "service@paypal.com <paypalonlinefundteam@mail2world.com>
To: [redacted]
Content-Type: multipart/alternative; boundary=001485f1d8989bd63f046f802ffb

--001485f1d8989bd63f046f802ffb
Content-Type: text/plain; charset=ISO-8859-1
Content-Transfer-Encoding: quoted-printable

[image: PayPal] <https://www.paypal.com/us>
```

- How can I check email? Cont’d
  - Hover the mouse over any links.



From: eFax.com <messages@inbound.efax.com>
Date: September 18, 2013, 10:35:20 AM CDT
To: <terry@coleinformatics.com>
Subject: eFax message from 15139880184 - 1 page(s), Caller-ID: 513-980-3082
Reply-To: <messages@inbound.efax.com>

eFax® Easy faxing anywhere.®

Fax Message [Caller-ID: 513-980-3082]

You have received a 1 page fax at 2013-09-12 06:56:56 CDT.

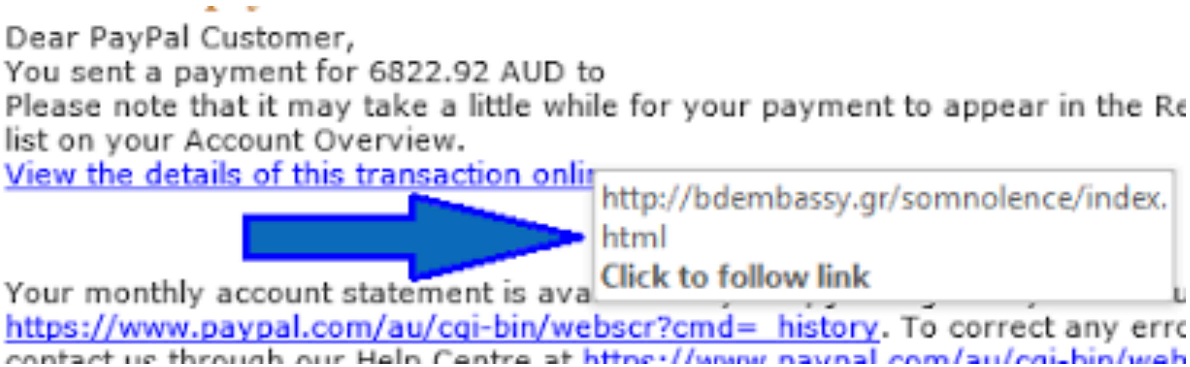
* The reference number for this fax is min1_did13-13 82-49.

View this fax online, on our website : http://www.efax.com/faxes/view_fax.aspx?fax_id=5139803082
Please visit www.eFax.com/en/efax/twa/page/help if you have any questions regarding this message or service.

http://www.jugurtha.be/
pdf_efax_5139803082.zip
Click to follow link

Actual Link!

- How can I check email? Cont’d
  - Beware of email or web addresses ending in two letters (.ru is Russia, gr is Greece, .be is Belgium, etc).



Dear PayPal Customer,
You sent a payment for 6822.92 AUD to
Please note that it may take a little while for your payment to appear in the Re
list on your Account Overview.
View the details of this transaction onli

http://bdembassy.gr/somnolence/index.html
Click to follow link

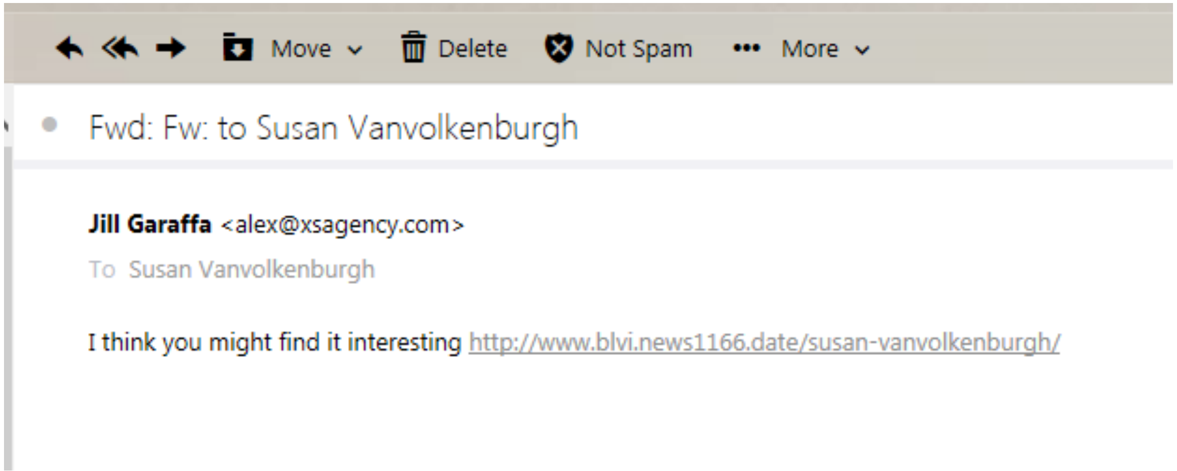
Your monthly account statement is ava
https://www.paypal.com/au/cgi-bin/webscr?cmd=_history. To correct any erro
contact us through our Help Centre at https://www.paypal.com/au/cgi-bin/web

- How can I check email? Cont’d
  - Think before you click.

- **Email Rules**
- Be sure who sent the email
- Never respond to “RE:” in the subject if you didn’t send the original. Delete it.
- Never click on a link until you knows where it goes.
- Be wary of links to pages ending in a two-character code indicating a foreign country.
- Never click on an attachment unless you know who sent and you were expecting it.
- Never follow sensationalized emails “Look what Donald Trump just said”.
- Always check the From against the Mailto:
- Check Sender against the From: in the header.

ASMC

- Hacked or Spoofed – What is the difference?
  - Hacked – Your email account has been compromised.
  - Spoofed – Someone is sending email with your name and/or your email address on it.



Fwd: Fw: to Susan Vanvolkenburgh

Jill Garaffa <alex@xsagency.com>

To Susan Vanvolkenburgh

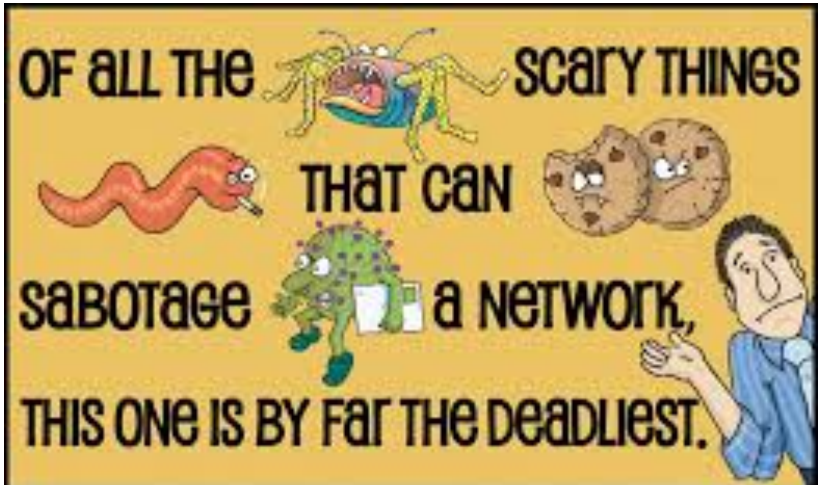
I think you might find it interesting http://www.blvi.news1166.date/susan-vanvolkenburgh/

- Hacked or Spoofed – How can I tell?
  - Hacked – If you received it, the mailto: will be from the hacked account. If you have been hacked you will most likely have emails in your sent items that you did not send.
  - Spoofed – The mailto: will not be the hacked account. If it supposedly came from you there will not be emails in your Sent items that you did not send.

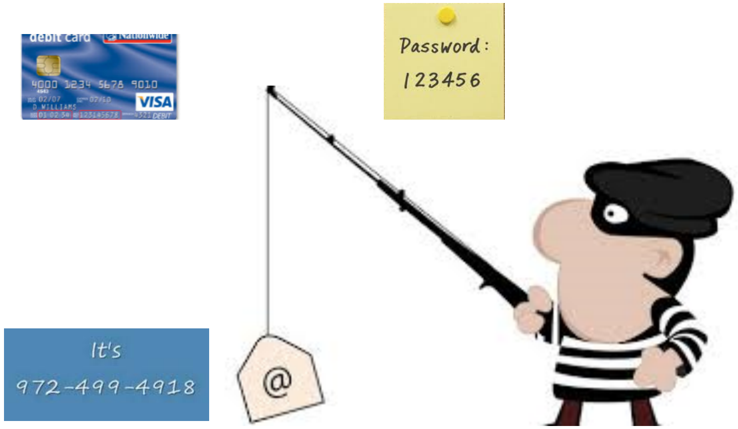
- Hacked or Spoofed – What can I do?
  - Hacked– Change your email password.
  - Spoofed—Change your email password. Maybe a new email address.
  - Notify everyone in your contacts of either incident.

I'm glad we're back in touch ever since I was spammed by your hacked email account.
someecards

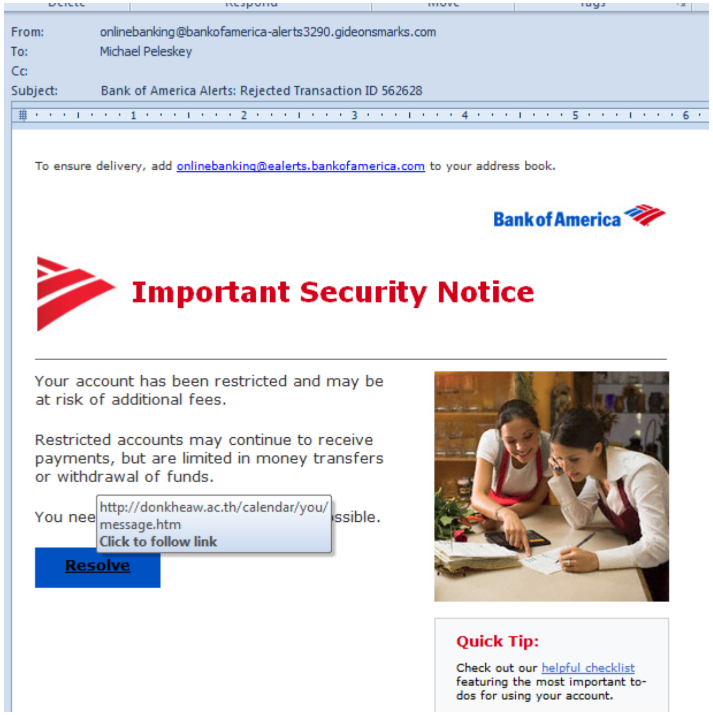
- Social Engineering - That means YOU!
  - Phishing
  - Vishing
  - SMishing



- Phishing
  - Ultimate aim is to gain access to private information:
    - Passwords
    - Account numbers
    - Phone numbers
    - Addresses
    - Birthdays



- Phishing emails that steal information want you to log in to a fake website made to look like the real website.



From: onlinebanking@bankofamerica-alerts3290.gideonsmarks.com
To: Michael Peleskey
Cc:
Subject: Bank of America Alerts: Rejected Transaction ID 562628

To ensure delivery, add onlinebanking@ealerts.bankofamerica.com to your address book.

Important Security Notice

Your account has been restricted and may be at risk of additional fees.

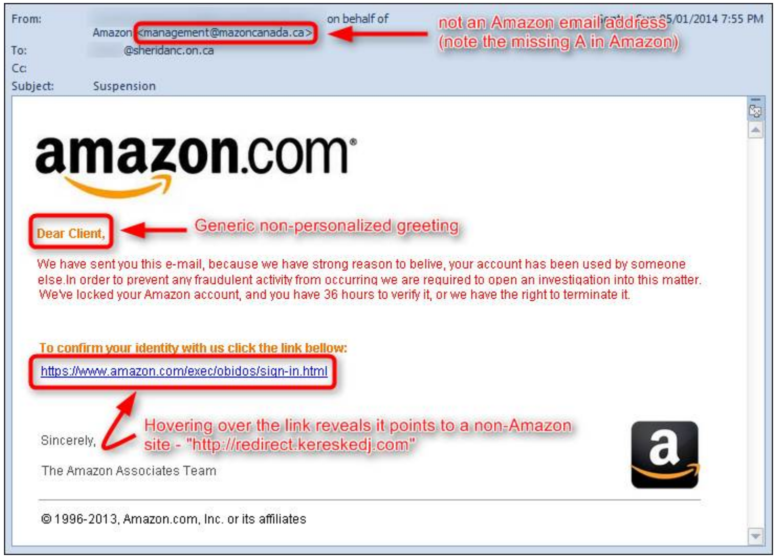
Restricted accounts may continue to receive payments, but are limited in money transfers or withdrawal of funds.

You nee http://donkheaw.ac.th/calendar/you/message.htm Click to follow link ssible.

Quick Tip:

Check out our helpful checklist featuring the most important to-dos for using your account.

- DO NOT FOLLOW ANY LINKS!
  - Go to the website in question by typing the web address into the browser address box.
  - Never use phone numbers or links provided in the email.



From: on behalf of Amazon <management@mazoncanada.ca>

05/01/2014 7:55 PM

To: @sheridanc.on.ca

Cc:

Subject: Suspension

not an Amazon email address (note the missing A in Amazon)

amazon.com

Dear Client,

Generic non-personalized greeting

We have sent you this e-mail, because we have strong reason to belive, your account has been used by someone else.In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter. We've locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it.

To confirm your identity with us click the link bellow:

https://www.amazon.com/exec/obidos/sign-in.html

Hovering over the link reveals it points to a non-Amazon site - "http://redirect.kereskedj.com"

Sincerely,

The Amazon Associates Team

© 1996-2013, Amazon.com, Inc. or its affiliates

- Vishing – Phishing over a telephone.
  - A call from a bank or credit card company saying your account has been compromised.
  - A call from Microsoft stating that they see you have problems and will help you fix them.
    - They will either ask for money or ask you to download something to infect your computer.
  - A call supposedly from a relative that is stuck overseas and needs money.

I'll need your card details
Your payment hasn't gone through
Please confirm your account password
I'm one of your suppliers

- How to combat Vishing:
  - Don't ever give personal information regarding banking or credit cards over the phone to someone who has called you.
  - If you get a call, hang up, and ring the number on the back of your credit card using a different phone from the one they called you on. The Vishers can hold your line so if you use your phone to call the account holder you will get the Visher back.

- Smishing – phishing text messages. Even your texts aren’t safe!
    - Often combined with Vishing, they may follow-up a text message with a phone call.
    - Unsolicited text messages with links should raise alarm bells.
    - If from a bank, call the bank using a number from a bank statement not a text message.

You have just won a $100 gift card! Click here to claim your gift.

- Identification – Are you really you?
  - Passwords
  - 2-Factor Authentication
  - Biometrics

- Passwords
  - The most common form of authentication.
  - The more complex the better.
  - 8 characters or more with capitals, non-capitals, numbers and symbols.

4

B

STARTING TODAY, ALL PASSWORDS MUST CONTAIN LETTERS, NUMBERS, DOODLES, SIGN LANGUAGE AND SQUIRREL NOISES.

g

- Passwords cont'd
  - – Password Keepers
    - Examples are LastPass and KeePass
    - Used because too many passwords to remember.
    - Some are cloud based and some are locally based.
    - Research which is right for you.

I forgot the password for the file where I keep all my passwords.

- Passwords-Top 10

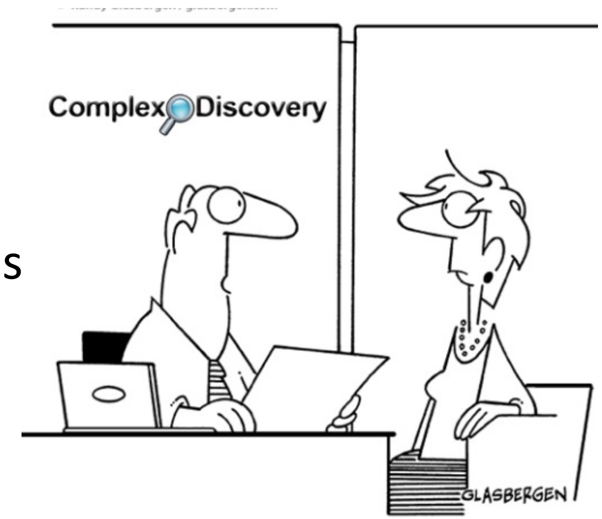
1. 123456
2. 123456789
3. qwerty
4. 12345678
5. 111111
6. 1234567890
7. 1234567
8. password
9. 123123
10. 987654321

[For Security Purposes, You Must Reset Your Password]
Enter Old Password: 12345
Enter New Password: 123456
I am a genius. There is NO WAY This account will EVER be hacked. I am amazed at my superior intellect.
1-30-2010

- How Passwords are cracked
  - Start with the top 25.
  - Guessing – based on predictability of using names and words that are familiar. May be gleaned from social networks.

"Yes, Fluffy was a great dog and to honor her memory, we've decided to keep her name as part of our computer password."

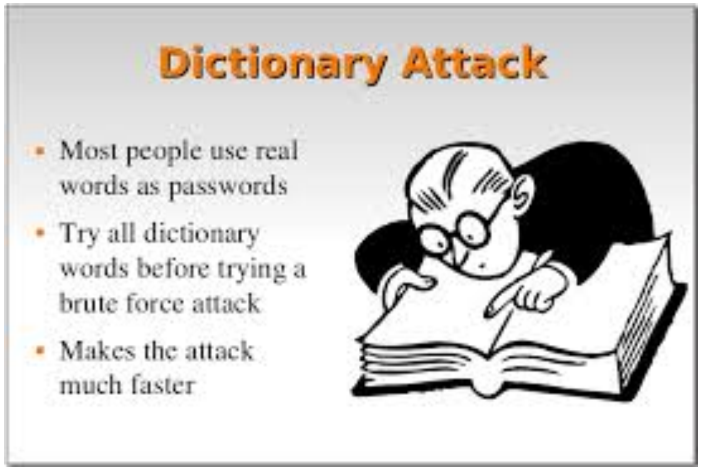
- Why Passwords are Cracked cont’d
  - Don’t think you have no reason to have your information stolen. Your identity is worth a lot of money.
    - Open new credit cards.
    - Rent and open utilities.
    - Counterfeit checks and ATM cards
    - Get driver’s license.
    - Get government benefits.
    - Sell your identity.



“Look at the bright side. Bad credit is your best protection against identity theft.”

- How Passwords are Cracked cont'd
  - Brute Force Attack – Tries every possible combination of characters at a rate of one hundred million per second.

- How Passwords are Cracked cont’d
  - Dictionary Attack – Assumes most passwords consist of whole words and dates.
  - Easier to crack then random numbers and letters.



Dictionary Attack

- Most people use real words as passwords
- Try all dictionary words before trying a brute force attack
- Makes the attack much faster

- How Passwords are Cracked cont’d
  - Phishing/Vishing/Smishing – just ask the person.
  - Exploits that people are eager to cooperate.

BEWARE OF SOPHISTICATED, HARD TO DETECT E-MAIL SCAMS
COOL!
SO GIVE ME YOUR ACCOUNT NUMBER, PASS-WORD, MOTHERS MAIDEN NAME AND I'LL GO HALVES WITH WHATEVER I GET
LYNCH

- 2 Factor Authentication
  - Login with a password then you are called or texted with a PIN.
    - Use for any financial institution and email.

Password
?
Login
+
Proof
Is that you?
✓
✕
=
Access
Success!

- Password Don’ts
  - DON’T Use easily guessed such as “password”. While it is no longer in the top two spots it is still on the top 10 and will be one of the first any hacker will try.

GOOD EVENING! YOUR PASSWORD PLEASE!
PASSWORD?!
PASSWORD ACCEPTED! WELCOME, MR. PRESIDENT. IT'S AN HONOR TO HAVE YOU HERE AGAIN!

- Password Don’ts cont’d
  - DON’T Use
    - Birthdays
    - SS#
    - Phone numbers
    - Family names
    - Information that is easily mined from social media sites

- Password Don’ts cont’d
    - DON’T Use same password or a slight variation at multiple sites. Once a hacker has one password he will try that same password or variations on it at other sites.

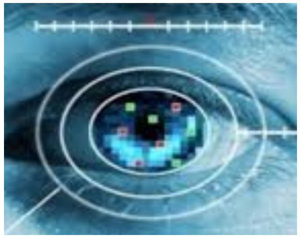
- Password Don’ts-Email Password
  - DON’T Use your email password anywhere else. Your email password is the keys to your kingdom. Every site has an option to reset your password. It sends the reset request to your email. Now the hacker can reset passwords to all your sites and lock you out!

This is something like The Lord of the PhoneRings
Why?
Because of that one password to rule them all.

- Password Don’ts
  - DON’T Use real information for security questions particularly your mother’s maiden name. Also change the information for each different site. If the website gets hacked your real information can be used for identity theft.

- Password Do’s
  - Password length 8-10 or greater
  - Use 2 Factor authentication (2FA)
  - Substitute numbers for letters-**l<n0tmyP3n$il**
  - First letter of each line of a specific page of a specific book. Password hint is name of the book –**WyoTcyeth** (welcome page of PRC handbook)
  - First line from a book-**0nc3uP0n@m1dnit3**

- Biometrics
  - Facial recognition
  - Fingerprints
  - Voice
  - Iris Scan
  - Keystroke dynamics
  - Lip Passwords
  - Privacy issues

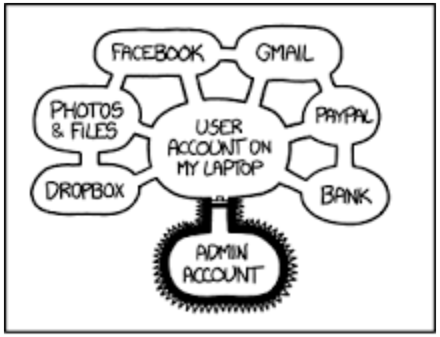


- Mobile Security
  - Multifaceted approach:
    - Physical security
    - WiFi security
    - Device password security
    - File password security
    - Virus scanning software

- Mobile Security cont’d
  - Do not walk away from a laptop, tablet or phone.
  - Mobile devices are easily stolen.
  - Computer locks can be cut.

- Mobile Security cont’d
  - Password protect data files on mobile devices.
  - Even if your device is password protected, password protect any sensitive files.

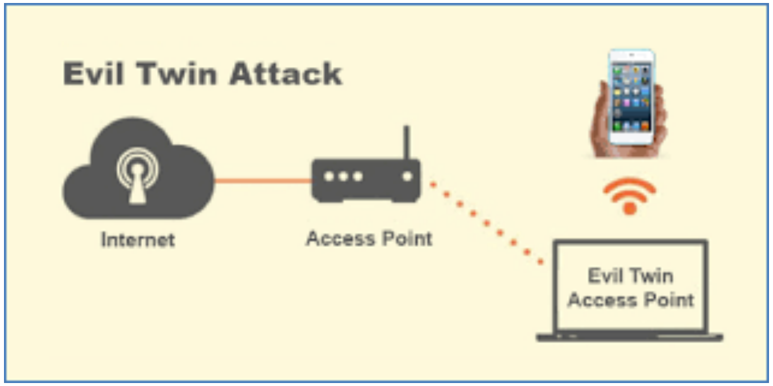
- Mobile Security cont'd
  - Password protect mobile devices.
  - Files aren't the only information that needs protecting.



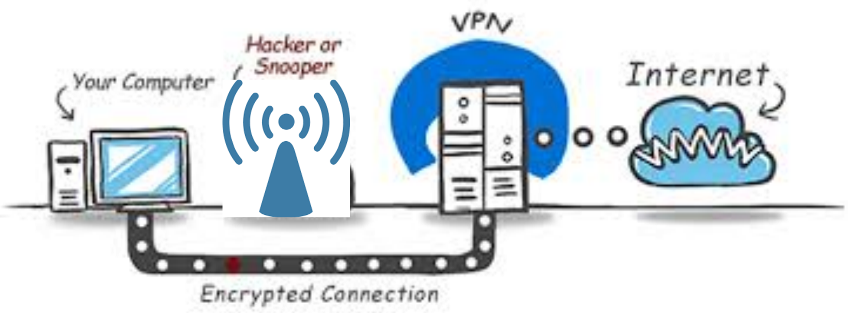
IF SOMEONE STEALS MY LAPTOP WHILE I'M LOGGED IN, THEY CAN READ MY EMAIL, TAKE MY MONEY, AND IMPERSONATE ME TO MY FRIENDS,

BUT AT LEAST THEY CAN'T INSTALL DRIVERS WITHOUT MY PERMISSION.

- Mobile Security cont'd
  - Don't access financial information in public using WiFi
    - Evil Twin
    - Set up in cyber cafés or where there is free WiFi.
    - You think you are using the café's access point but you are on an Evil Twin access point.
    - Used to intercept passwords and private information.



- Mobile Security cont'd
  - Use cellular data for financial and sensitive info or a VPN.
    - Cellular data is not subject to man-in-the-middle attacks.
    - VPN creates a private network using software



- Mobile Security cont’d
  - Watch who is looking over your shoulder
    - Shoulder Surfing
    - Watch who is doing what with a selfie stick and their cellphone.

"FREE PUBLIC WIFI"? OBOY!
CLICK
A FOOL AND HIS PASSWORD ARE SOON PARTED.

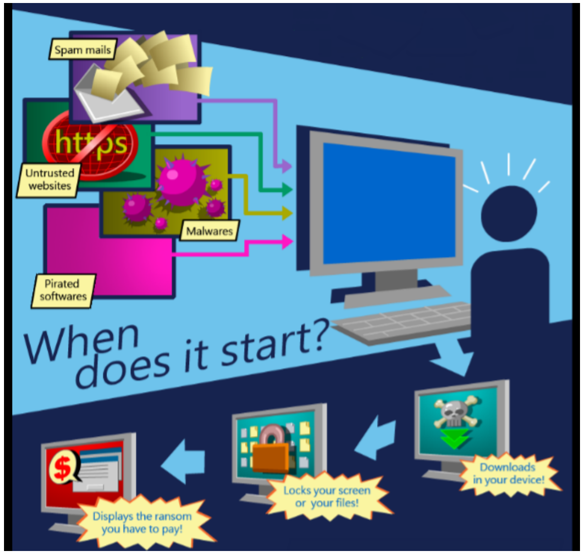
- Mobile Security cont’d
  - Mobile device viruses.
  - Many apps infected.
  - Install virus scanning app.
  - Be careful what you download particularly games.

- Ransomware
  - Virus that encrypts your files and/or your hard drive and demands money to restore it.
  - Do not pay the ransom. No guarantee the data will be restored.
  - Only defense is a good backup.

- How do you get Ransomware
  - By clicking on an infected popup ad.
  - By visiting an infected site.
  - By clicking on an email link or attachment.

click!

click!

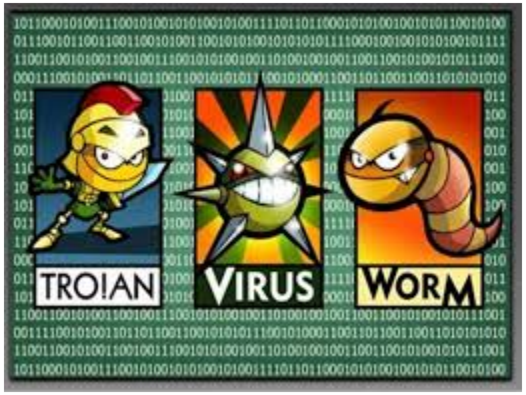

Spam mails
https
Untrusted websites
Malwares
Pirated softwares
When does it start?
Downloads in your device!
Locks your screen or your files!
Displays the ransom you have to pay!

click!

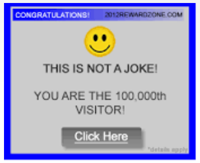
click!

- What can you do about Ransomware
  - Use a reputable anti-virus software and firewall.
  - Back up all of your computer data.
  - Don’t click on suspicious links.
  - Keep all installation discs or make rescue discs.
  - If you get it disconnect from the Internet.

- Malware
  - Most common form of computer ailments
    - Virus
    - Worms
    - Trojan Horses
    - Spyware
    - Adware
    - Scareware



- Malware cont’d
  - How did I get malware?
    - Accepting without reading popups
    - Downloading software
    - Opening email attachments
    - Visiting unknown links
    - No anti-virus software

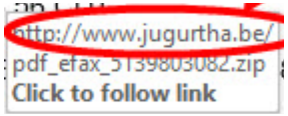


CONGRATULATIONS! 2012REWARDZONE.COM

THIS IS NOT A JOKE!

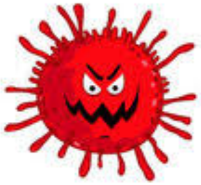
YOU ARE THE 100,000th VISITOR!

*details apply



http://www.jugurtha.be/
pdf_efax_5139803082.zip
Click to follow link

- Viruses
  - A virus almost always corrupts or destroys data.
  - Spreads to other computers by sharing files or sending emails with attachments.
  - Viruses need you to spread.

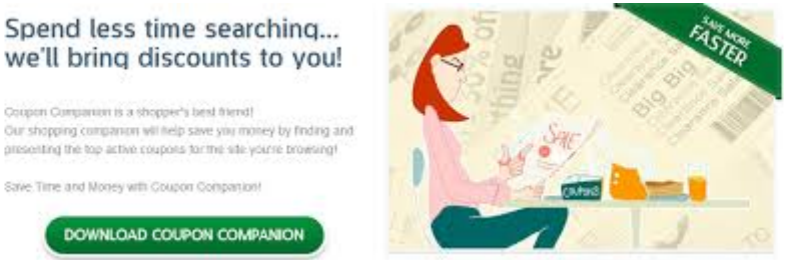


- Worms
  - Usually downloaded via an email attachment.
  - Replicate functional copies of themselves.
  - Can cause the same type of damage as viruses.
  - Do not require a host program or human help to propagate.
  - Often install a backdoor on a computer system so it can be remotely controlled making the computer a “zombie”.

- Trojan Horses
  - Named after the wooden horse the Greeks used to infiltrate Troy.
  - Harmful piece of software that looks legitimate.
  - Popping up windows or changing desktops.
  - Deleting files, stealing data, or activating and spreading other malware, such as viruses.
  - Do not replicate.
  - Create back doors to give malicious users access to the system.

- Spyware
  - Gathers information and transmits it to third parties.
  - Steals confidential data, passwords, etc.
  - Designed to stay hidden so that it can steal information from you.
  - Browser add-ons.
  - Drive-by download through a pop-up.
  - Masquerades as anti-spyware.

- Adware
    - Form of Spyware
    - Displays ads when you're connected to the internet.
    - Infects your computer with unwanted advertising, including pop-up ads.
    - May conceal more malicious types of spyware as well. Includes Browser hijackers.
    - Often bundled with legitimate software

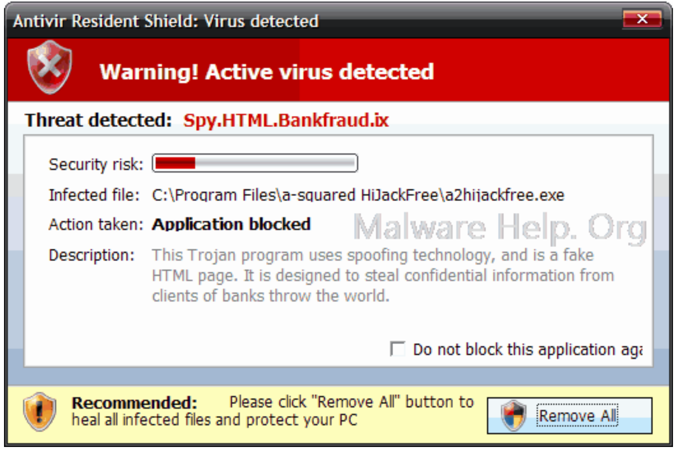


Spend less time searching...
we'll bring discounts to you!

Coupon Companion is a shopper's best friend!
Our shopping companion will help save you money by finding and presenting the top active coupons for the site you're browsing!

Save Time and Money with Coupon Companion!

- Scareware
  - Designed to sell you a product by falsely telling you that your security is out of date, your computer is already infected.
  - May implant malware just so it can sell customers a program that promises to “fix” the problem
  - Could steal your credit card information
  - May purport to be from Microsoft



Antivir Resident Shield: Virus detected

Warning! Active virus detected

Threat detected: Spy.HTML.Bankfraud.ix

Security risk:

Infected file: C:\Program Files\a-squared HiJackFree\a2hijackfree.exe

Action taken: Application blocked

Description: This Trojan program uses spoofing technology, and is a fake HTML page. It is designed to steal confidential information from clients of banks throw the world.

□ Do not block this application aga

Recommended: Please click "Remove All" button to heal all infected files and protect your PC

- Keylogging
  - Malicious program that covertly tracks each keystroke typed by the computer’s owner. Keylogging is an example of spyware that’s typically used to steal user passwords.

- Web Safety
- Avoid questionable Web sites
- Only download software from sites you trust. Carefully evaluate free software and file-sharing applications before downloading them.
- Update your operating system regularly
- Increase your browser security settings
- Type in a trusted URL for a company's site into the address bar of your browser to bypass links in an email or instant message
- Make sure that you have the best security software products installed on your PC:
  - Use antivirus protection and a firewall
  - Get antispyware software protection

- Social Media
  - Facebook Scams
  - Too Much Information
  - Malware ridden comments

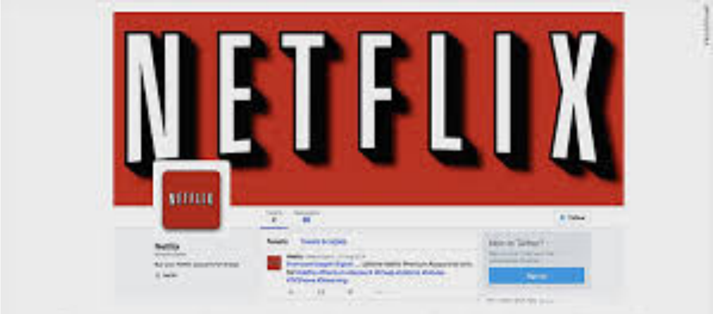
- Social Media Scams
  - Chain Letters
    - "Retweet this and Bill Gates will donate $5 million to charity!"
    - A child is sick and cannot afford the surgery.
    - A new virus is going around. Go here to protect your computer.
    - If you send this chain letter you will get money.
    - If you don't send this to 10 people bad things will happen.
    - Check all of these on Snopes.com

- Social media Scams
  - Cash Grabs
    - You just received an urgent request from one of your real friends who "lost his wallet on vacation and needs some cash to get home."
    - May also be a phone call.
    - Call the friend or relative that needs “Help”.

Dear Sue,
Help!1!!! Please to send $2,000 via wire transfer.
Your friend,
Jill

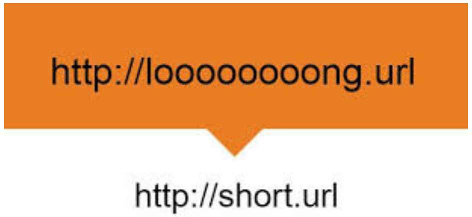
- Social Media Hidden Charges
  - What type of STAR WARS character are you? Find out with our quiz! All of your friends have taken it!"
  - You are neither Yoda or Darth Vader. You are Sucker.
  - Subscribes you to a service billed to your cell phone.
  - That "free, fun service" is neither. Be wary of these bait-and-switch games. They tend to thrive on social sites.

- Social Media Phishing Requests
  - Fake customer service accounts
  - Fake comments on popular posts
  - Fake live-stream videos
  - Fake online discounts
  - Fake online surveys and contests.



Fraudsters create fake social media accounts for real businesses like Netflix to carry out financial phishing scams.

- Social Media Hidden URL’s
  - Beware of blindly clicking on shortened URLs.
  - Everywhere on Twitter, hides the full location. Link could install all sorts of malware on your computer.
  - Not easily checked. Use CheckShortURL.
  - Try searching using Google for where the link is supposed to go.

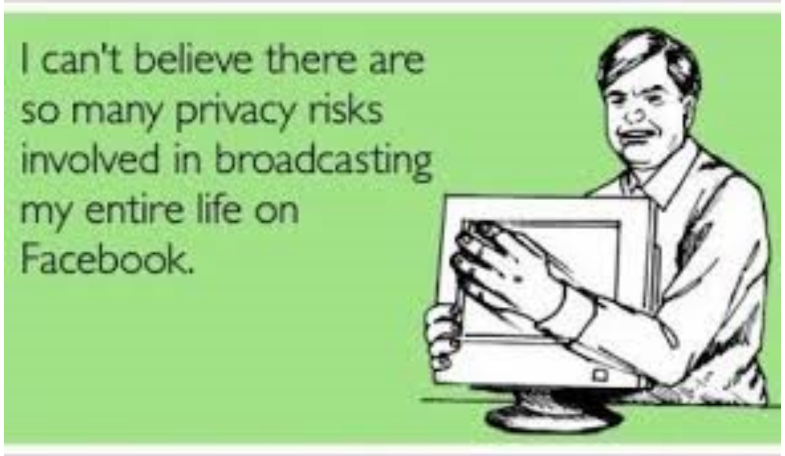


http://looooooong.url

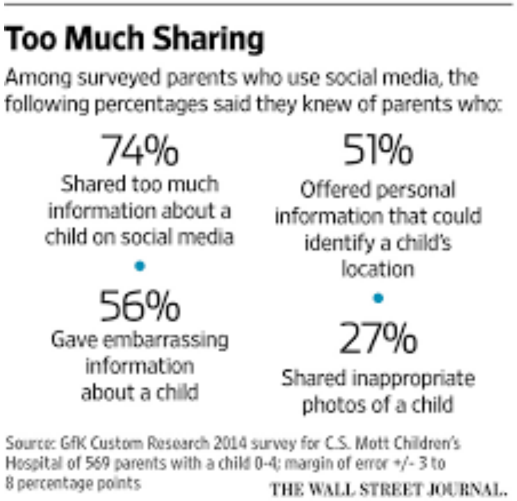
http://short.url

- Social Media Malware infected comments
  - Receive a notification about a friend tagging in a comment.
  - Clicking the link, a malware file is downloaded.
  - Click the downloaded file and infect the devices.

- Too Much Information
  - Don’t put your address and phone number on Facebook!
  - Perverts love social media.
  - Thieves Love social media.
  - Lawyers Love social media.
  - Private detectives love social media.


I can't believe there are so many privacy risks involved in broadcasting my entire life on Facebook.

- Too Much Information cont’d
  - Perverts love Facebook –
  - Limit the number of photos of your kids.
  - Limit information about them.
  - Limit information on where they are when.



Too Much Sharing

Among surveyed parents who use social media, the following percentages said they knew of parents who:

74%
Shared too much information about a child on social media

56%
Gave embarrassing information about a child

51%
Offered personal information that could identify a child’s location

27%
Shared inappropriate photos of a child

Source: GfK Custom Research 2014 survey for C.S. Mott Children’s Hospital of 569 parents with a child 0-4; margin of error +/- 3 to 8 percentage points

THE WALL STREET JOURNAL.

- Too Much Information cont’d
  - Stalkers love Facebook –
  - Limit the number of photos of you looking sexy.
  - Limit information about yourself – Status goes from “in a relationship” to “Single”. The people who count already know.
  - Limit information on where you are when.

- Too Much Information cont’d
  - Thieves Love Facebook –
  - Just "checked-in" at the local gym
  - Start our week’s vacation in Mexico tomorrow.
  - Just checked in at the bar in Cabo!
  - This would be a great time to rob you.
  - Post pictures of your trip after you are home.

Cyber Security
HURRY UP, THEIR FACEBOOK PAGE SAYS THEY ARE RETURNING FROM VACATION TOMORROW!

- Too Much Information cont’d
  - Lawyers Love Facebook –
  - Anything you post on Facebook can and may be used against you in a court of law.
  - Wealth of information for lawyers on both sides of a case.
  - What is posted can be enough to bring a case.

SUBPOENA

To (name)

of (address)

State: Postcode:

YOU ARE ORDERED TO: (select one box

□ Attend court to give evidence (see Part A of order)

□ Attend court to give evidence and produce doc Part B for details of order)

□ Produce documents to the Court (see Part C for deta

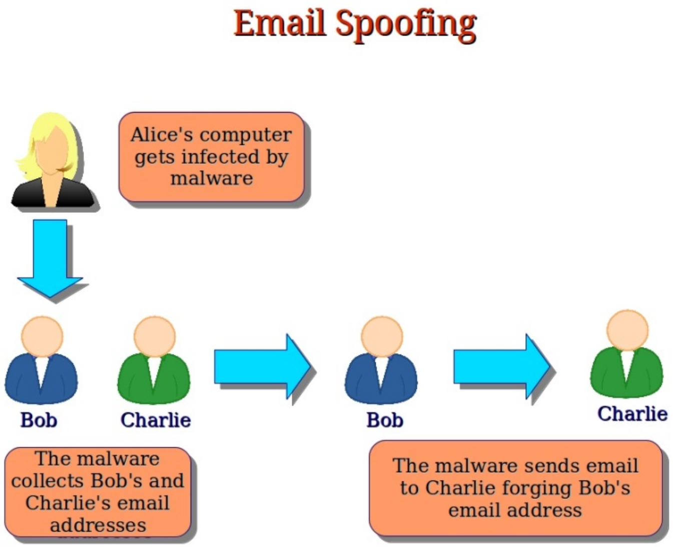
TAKE NOTICE: IF YOU FAIL TO OBEY THIS SUBPOE
a warrant may issue for your arrest
you may be liabl

- Hacked Information
  - Has my information been hacked
  - Large data breaches
  - The below website will check to see if your information has been caught in a data breach
    - Haveibeenpwned.com

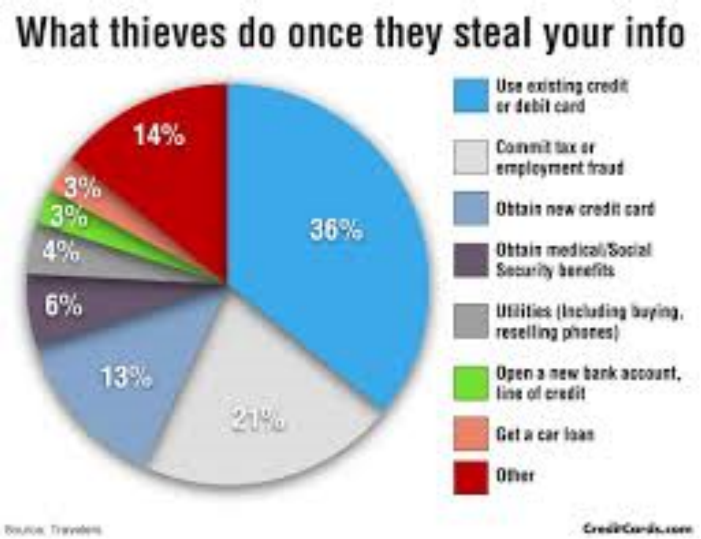
Hackers hit
"What's been taken is bits of data that the ... put together into an identity."

- Cyber Myths
  - I don’t need security software, I don’t access unsafe sites.
    - Cyber attackers are able to exploit safe websites and insert malware into their ads and then into your system.
    - **You can access a safe, perfectly legitimate website that doesn’t even require you to click on something and still get infected.**

- Cyber Myths cont'd
  - **I only open emails from my friends, so I'm safe.**
    - See the sections on email, hacked, spoofed.


Email Spoofing
Alice's computer gets infected by malware
Bob
Charlie
Bob
Charlie
The malware collects Bob's and Charlie's email addresses
The malware sends email to Charlie forging Bob's email address

- Cyber Myths cont’d
  - **I Don’t Have Anything Worth Stealing**
    - Health data.
    - Sensitive data you don’t want anyone to know.
    - Personal information for identity theft.



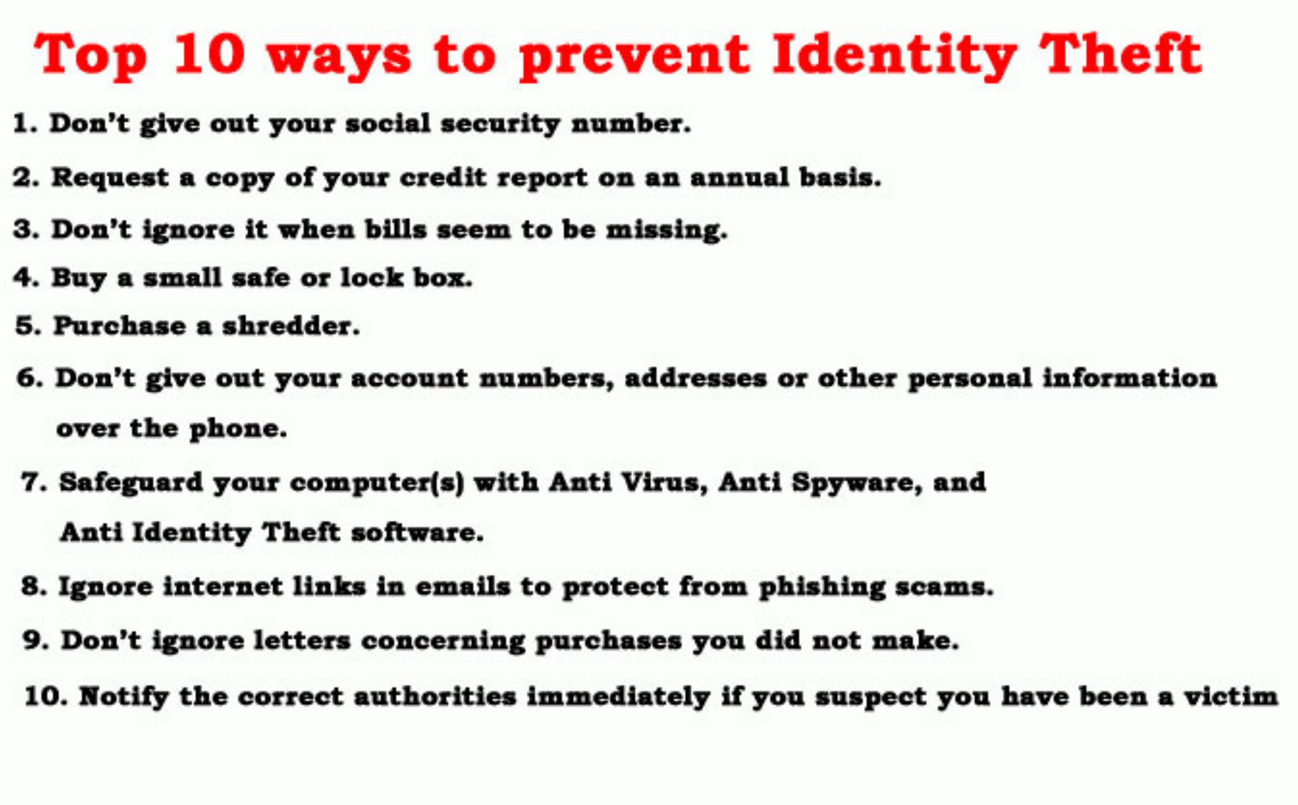
What thieves do once they steal your info

Source: Travelers

CreditCards.com

- Prevent Identity Theft
  - – Unless for a bank or financial institution never use real information.
    - Don’t use your real birthday.
    - Don’t use real information such as your mother’s maiden name.

- Prevent Identity Theft



Top 10 ways to prevent Identity Theft

1. Don't give out your social security number.
2. Request a copy of your credit report on an annual basis.
3. Don't ignore it when bills seem to be missing.
4. Buy a small safe or lock box.
5. Purchase a shredder.
6. Don't give out your account numbers, addresses or other personal information over the phone.
7. Safeguard your computer(s) with Anti Virus, Anti Spyware, and Anti Identity Theft software.
8. Ignore internet links in emails to protect from phishing scams.
9. Don't ignore letters concerning purchases you did not make.
10. Notify the correct authorities immediately if you suspect you have been a victim

- IoT – Internet of Things
  - Inter-networking of physical devices.
    - Internet aware.
      - Smart thermostats.
      - Amazon Echo or Google Home.
    - Accesses the Internet through a router.
    - Estimated 24 Billion IoT devices by 2020

www.jklossner.com
klossner
"WE HAVE TO GO OUT FOR DINNER. THE REFRIGERATOR ISN'T SPEAKING TO THE STOVE."

- IoT – Internet of Things cont’d
  - – Security
    - Same rules as your computer.
    - Strong router password.
    - Strong Wi-Fi password.
    - Strong device password if it has one.
    - Accesses the Internet through a router.

- Dangerous Snail Mail
  - Pre-filled In Credit Card Applications
  - Pre-filled In Insurance Applications
  - Credit card bills
  - Any financial mail with account numbers
  - Address Fraud
  - Home Title Theft-usually on a 2nd home

- Dangerous Snail Mail-Cont’d
  - All Pre-filled Applications can be used to take out credit cards or Insurance in your name.
  - Can use your credit cards with the account number.
  - Can use your information to get a driver’s license.
  - Can use your information to file fraudulent documents to get title to your house.
  - SHRED ANYTHING WITH AN ACCOUNT NUMBER

- Cyber Security in Summary
  - You are your biggest vulnerability and your best defense.
    - The bad guys are out to get you.
    - Trust nothing.
    - Do not click if you are not sure.
    - Protect your information.

    Think before you click.