Cybersecurity

Heber Slusser

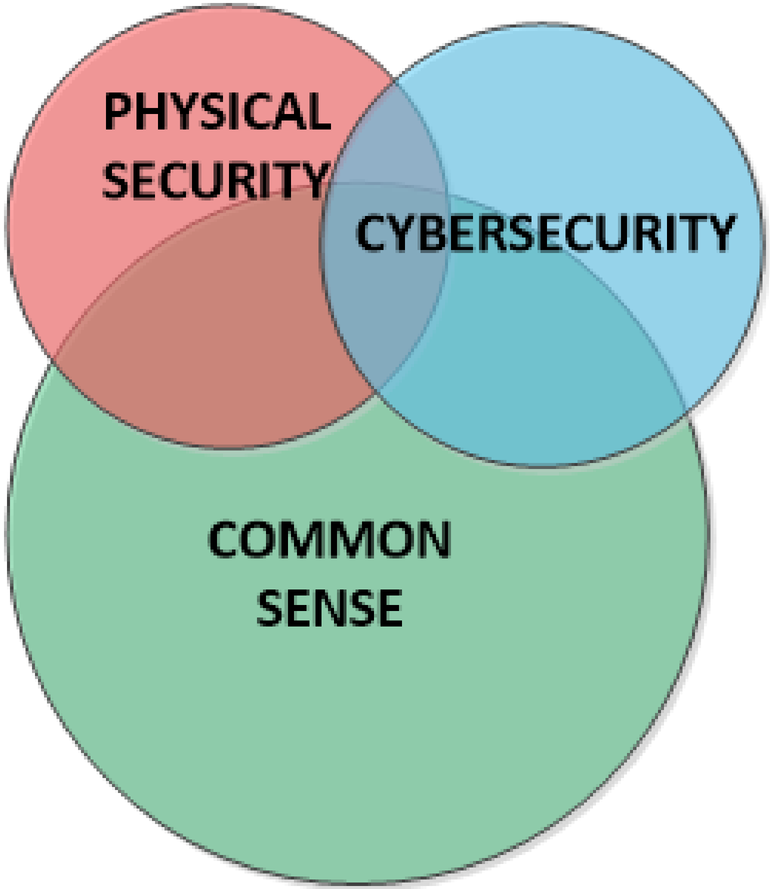
SIR Branch 62

What is Cybersecurity?

- **Computer security, cybersecurity is the protection of computer systems from theft or damage to their hardware, software or electronic data, as well as from disruption or misdirection of the services they provide.**

From Wikipedia, the free encyclopedia

3 Elements of Security



Physical Security

- Keep your devices secure
- Don’t leave your phone in your car – Bluetooth and WiFi can be detected outside of your car saying “Here I Am – Take Me!)
- Password lock all computing devices
- Consider enabling tracking on your phone to find it if lost
- Keep a written copy of passwords
- Keep track of thumb drives with security stuff on them
- Be aware of your surroundings

Exposing Information Publicly

SIR
©
SOCIAL ACTIVITIES FOR MEN

2024

Membership Directory

Sunnyvale
Branch 62

Share With Care

- **What you post will last forever:** Be aware that when you post a picture or message online, you may also be inadvertently sharing personal details with strangers about yourself and family members – like where you live
- **Post only about others as you would like to have them post about you:** The golden rule applies online as well
- **Own your online presence:** It's OK to limit who can see your information and what you share. Learn about and use privacy and security settings on your favorite websites

Passwords

Please tell me you're not adding a special cymbal to your password.
Blazek
10-21

Get this cartoon signed & framed & get signed LP books at LoosePartsComic.com
©2021 Dave Blazek · looseparts@verizon.net · Washington Post News Service & Syndicate

WHY?

Re-used passwords can lead to compromised financial accounts 😰

- **Protects Personal Information**
- **Prevents Unauthorized Access: Safeguards Your Identity: Prevents Account Hijacking**
- **Mitigates Risk of Hacking:**
  - **Protects Against Phishing**
  - **Reduces Impact of Data Breaches**
  - **We know some of us have had our e-mail accounts hacked**
- **Ensures Privacy**
- **Maintains Confidentiality**
- ***Avoids the Hassle of Recovery***

How to Create a Strong Password

- Use a “Pass Phrase” – 3 to 5 random words strung together such that you can remember them
  - DeskF1uffyWa!! (DeskFluffyWall) (15 characters)
- Use “First Letter” – use the 1st letter of each word in a phrase or song
  - "When you're weary, feeling small,
    When tears are 1n your eyes, ! will dry them all.“
  - WywfsWta1ye!wdta (16 characters)
- Use a password generator like Norton

P@ssw0rd – Replacing a few letters with symbols doesn’t create any real degree of complexity.

Strong Password?

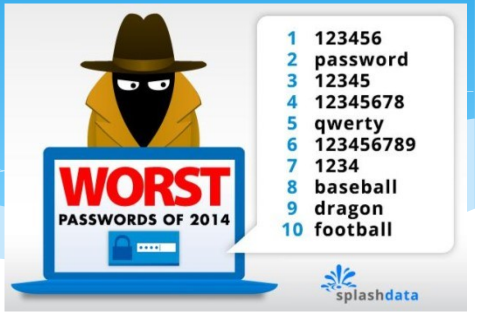
- Hypothetically (14 characters)
- Hypothetic/\11y (15 characters)
- O#_qh6W8 (8 characters)
- correcthorsebatterystaple (25 characters)
- Correct-horse2battery (21 characters)
- WywfsWta1ye!wdta (16 characters)

Password Dictionary

- Don’t use a word in the dictionary for a password
  - Hacking software uses dictionaries (foreign ones too!)

- Don’t use a family name (or anyone’s name)

Most Common Passwords



1 123456
2 password
3 12345
4 12345678
5 qwerty
6 123456789
7 1234
8 baseball
9 dragon
10 football

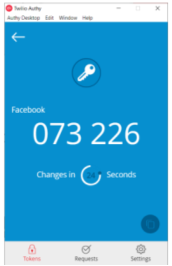
123456	23.2 million accounts
123456789	7.7 million
Qwerty	3 million
Password	3 million
111111	
12345678	
abc123	
1234567	
password1	
12345	

Recently, some 32 million passwords were stolen from social-networking service RockYou and released into the wild by the hacker who nabbed them

- "iloveyou" just missed out on the top 10, while "monkey“, and "dragon" made surprise appearances in the top 20 - “FuckYou” (#40),
- Ashley and Michael were the most common names used, followed by Daniel, Jessica and Charlie.

Two-Factor Authentication (2FA)

- Text message code (good)
- Authenticator app code (better)
  - Application that generates time-based one-time passwords (TOTP) for the purpose of multi-factor user authentication



Facebook

073 226

Changes in 24 Seconds

- Hardware security key (best)

Where to Store Passwords

- Password manager
  - – Generates and stores passwords in an encrypted vault
  - – Automatically fills passwords into websites
  - – Bitwarden, 1Password, Dashlane, Keychain
- Passkey (WebAuthn, FIDO2)
  - Sign in to apps and websites with a biometric sensor (such as a fingerprint or facial recognition), PIN, or pattern, freeing them from having to remember and manage passwords.
- Google, Facebook, eBay, Microsoft, Apple
- A written list (hard copy)

Password Managers

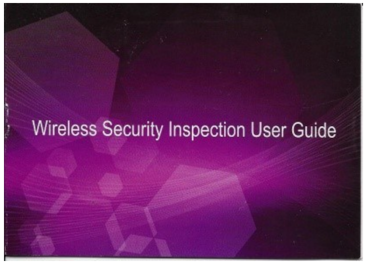
- BitWarden
- 1Password
- Daslane
- Enpass
- Keeper
- LogMeOnce
- RoboForm
- Sticky Password

Don’t Reuse Passwords!

Example:

- Your WiFi router password is hacked (EASY!)
- It is the same password as you use for your email
- You get an email from your bank
- Your bank has the same password

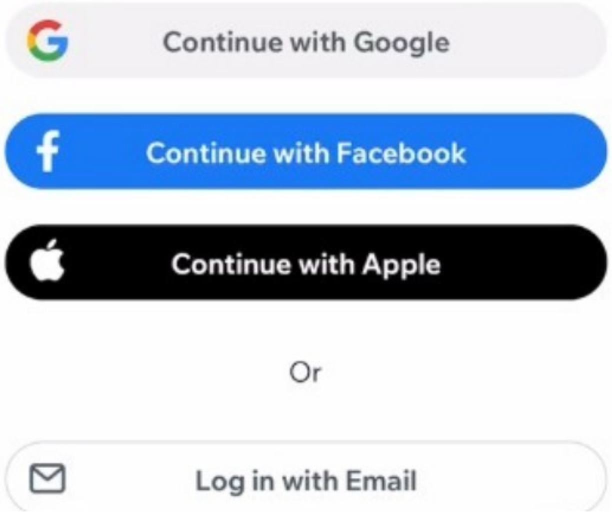
- On and on …



WiFi hacking software that came with a WiFi antenna

Same Password for Different accounts?

- Use Single sign-on (SSO) only if you:
  - Enable – and we can’t stress this enough – two-factor authentication (2FA) on the primary account, as this will make it harder for anyone to impersonate you online,
  - Trust the platform you’re using to access the other website – trust is a fickle thing, however, and you still need to take other precautions,
  - Use payment services like PayPal or a virtual credit card as payment options for any website you accessed using SSO; this will help you avoid leaking your banking details,
  - Use the settings in your primary account to keep track of all the websites you’ve linked it to.



Common Sense

- This is a tough one
- If it appears to be too good to be true … It probably is.
- If you didn't originate the conversation with a stranger, be very suspicious

SIR

Living Longer & Happier

AARP®

Fraud Watch Network

[AARP Fraud Information Link]

Fraud

PHISHING
depositphotos

WHAT GREAT FREE APPS YOU HAVE, GRANDMA!
ALL THE BETTER TO HARVEST YOUR PERSONAL DATA, BUILD UP MY TECH FIRM AND ONSELL FOR BILLIONS
SLANE

Fraud - Telephone

- Incoming – You have been selected for ???
- Outgoing – the number provided on the internet isn't going to the place that you had intended (DMV -> auto insurance)
- Your loved one is in jail …
- I'm out of town and need to send a gift card to …
- Robo Calls – A pain. Consider using NoMoRobo for your land line (not for cell phones)
- Use your SPAM filter on your Smart Phone

Fraud - Email

- Spam
  - Use your Spam filter – block unwanted emails
  - Do the same thing for Text Messages
- Send money to …
  - Be really careful before you send $. *Ask a friend if it sounds real – two heads are sometimes better than one*
  - Contact the recipient using your own contact information to verify the validity of the request

Fraud – Hacked Accounts

- Every now and then we get a report that some of our data has been hacked from xyz company and we are, therefore, subject to fraud
- We have all received email from someone that we know that wants $ but it isn’t really that person. It is most likely that the “senders” email password was hacked – use better passwords!

Phishing (Social Engineering)

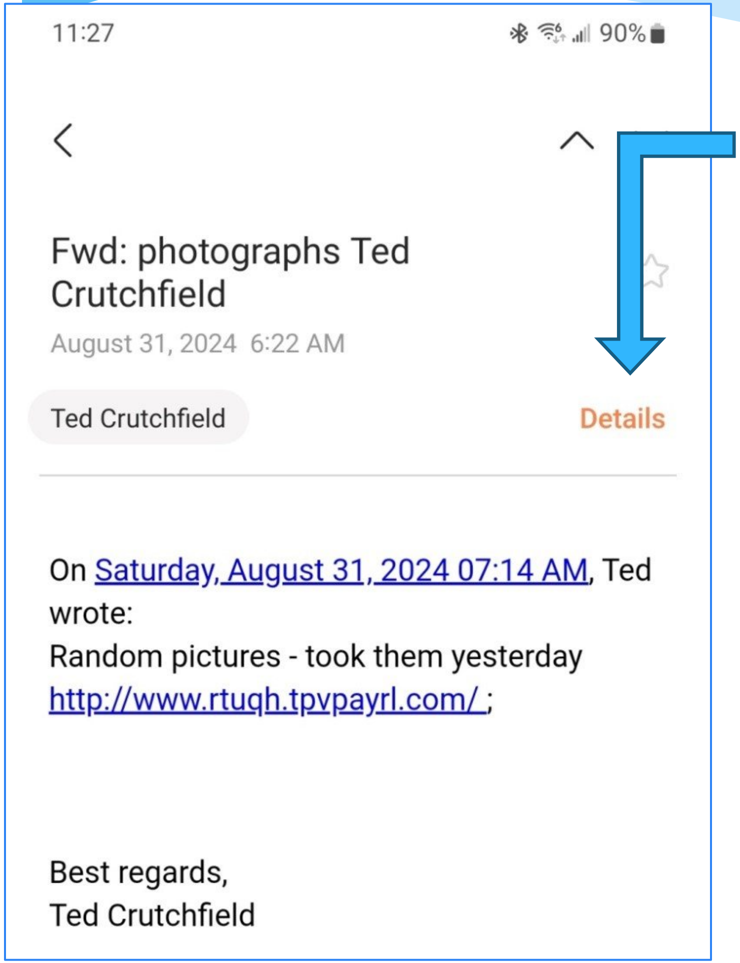
The phisher wants to trick us into doing something

- A stranger initiated the conversation
- Authority figure
- Urgency
- Send money (eventually)

Spear Phishing

Spear phishing is a type of phishing attack that targets a specific individual, group or organization. These personalized scams trick victims into divulging sensitive data, downloading malware or sending money to an attacker

Received Phishing E-mail



11:27 90%

Fwd: photographs Ted Crutchfield

August 31, 2024 6:22 AM

Ted Crutchfield

Details

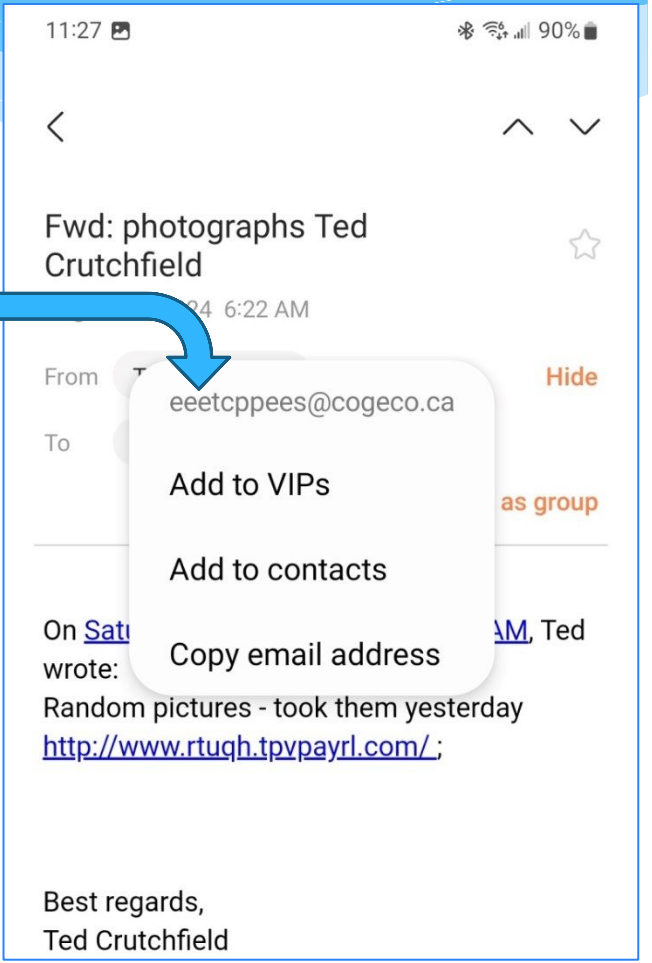
On Saturday, August 31, 2024 07:14 AM, Ted wrote:
Random pictures - took them yesterday
http://www.rtugh.tpvpayrl.com/ ;

Best regards,
Ted Crutchfield

Click Details

Click From Name

Does it look REAL??



11:27 90%

Fwd: photographs Ted Crutchfield

24 6:22 AM

From

To

Hide

as group

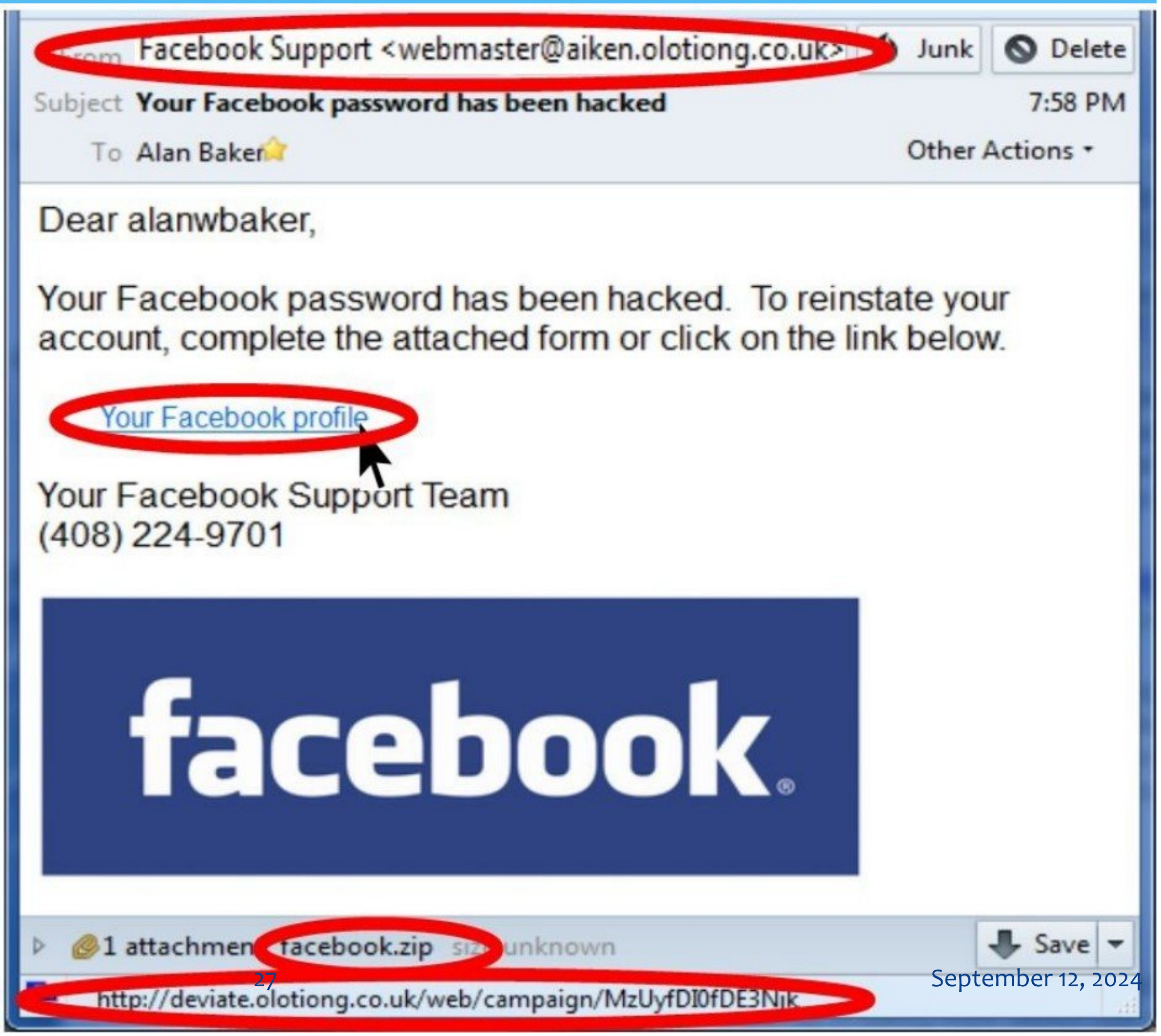
eeetcppees@cogeco.ca

On Sat AM, Ted wrote:
Random pictures - took them yesterday
http://www.rtugh.tpvpayrl.com/ ;

Best regards,
Ted Crutchfield

Phishing Email’s Red Flags

- From address
- Link address
- Attachment



rom Facebook Support <webmaster@aiken.olotiong.co.uk>

Subject **Your Facebook password has been hacked** 7:58 PM

To Alan Baker

Dear alanwbaker,

Your Facebook password has been hacked. To reinstate your account, complete the attached form or click on the link below.

Your Facebook profile

Your Facebook Support Team
(408) 224-9701

facebook.

1 attachmen facebook.zip siz unknown

http://deviate.olotiong.co.uk/web/campaign/MzUyfDI0fDE3Nık

Who Can Be Cheated?

- Greed can make people vulnerable to scams
- When driven by greed, common sense often fades
- Many are willing to risk small losses for the promise of bigger gains
- People seek shortcuts to achieve difficult goals
- Desire for wealth without effort makes individuals easy targets
- Scammers exploit these greed-driven tendencies
- It's hard to cheat someone who isn't motivated by greed
- Similar to greed, love can cloud common sense

What is ID Theft?

- Identity theft or identity fraud happens when a thief gains access to personal information like your name, address, credit card or bank account numbers, Social Security number, phone or utility account numbers, passwords, or medical insurance numbers—and uses that information for their economic gain

Is this a REAL Problem?

- Some 32.9 million consumers were victims of identity theft in 2021, with combined losses equaling $16 billion*
- FTC reported that 29 percent of identity theft victims indicated that their data was used to commit tax fraud

This is a hard number to verify. Lots of sources have lots of different information.

How Effective are the Thieves?

- U.S. Fraud and Identity Theft Losses Topped $10 Billion In 2023 (Experian)
- Shape Security says credential stuffing attacks can be effective as often as 3% of the time. It may not seems like a large number of successful logins, but that's 30,000 wins for every million attempts

Credential stuffing is a cyberattack where a malicious actor uses stolen credentials to gain access to multiple accounts. This type of attack is based on the assumption that people often use the same usernames and passwords for different accounts.

Top Five Types of Identity Theft Fraud, 2023

Category	Number of Complaints
Imposter scams	856,284
Online shopping and negative reviews	376,460
Prizes, sweepstakes and lotteries	158,070
Investment-related scams	110,388
Business and job opportunities	108,459
Internet services	102,105
Telephone and mobile services	97,052

How Common are Identity Theft Attacks?

- These attacks are much more common than you might think. According to Shape Security, around 90% of all login attempts on retail websites aren't shoppers logging in with their own accounts. They're the result of a credential stuffing attack
- Other kinds of sites are targeted, too. Airline sites come in second, where credential stuffing accounts for about 60% of logins. Just behind airlines are online banking sites at 58%. Rounding out the top four: hotels at 44%

Credential stuffing is a cyberattack where a malicious actor uses stolen credentials to gain access to multiple accounts. This type of attack is based on the assumption that people often use the same usernames and passwords for different accounts.

Prevention – Credit Freeze

- *Place a Credit Freeze at each credit bureau – IT IS FREE!*
- You probably are not getting new credit cards, buying a house, or a car on a regular basis
- You can “Un-Freeze” in minutes if required
- Online or by phone
  - Equifax
  - Experian
  - TransUnion

Get a Free Credit Report

- You can have 1 free report every 12 months from each nationwide credit bureau:
  - Equifax: 1-800-685-1111; Equifax.com/personal/credit-report-services
  - Experian: 1-888-397-3742; Experian.com/help
  - TransUnion: 1-888-909-8872; TransUnion.com/credit-help

Place a Fraud Alert

- Contact one of the three credit bureaus. That company must tell the other two.
  - TransUnion.com/credit-help
    888-909-8872
  - Experian.com/help
    888-EXPERIAN (888-397-3742)
  - Equifax.com/personal/credit-report-services
    800-685-1111

Hackers Can Take Advantage of You and Your Information.

- Your info could be used to open credit cards or take out loans.
  - Social Security number, name, birthdate and address
- Hackers can intercept your tax refund.
  - Social Security number, name, birthdate
  - File a bogus tax return before you do
- Your info can be used to cover medical treatment.
  - Social Security number and health insurance account numbers. address, phone number…
- Hackers can take flights with your airline miles.
  - Airline miles can be converted to cash by easily going to websites that buy miles
- Your info could be used to open utility accounts.
  - run up tabs on the account, which is under your name
- Infest your computer with a virus, trojan, worm, or bot.

What To Do Right Away

- Step 1: Call the companies where you know fraud occurred
- Step 2: Place a fraud alert and get your credit reports
- Step 3: Report identity theft to the FTC

You may choose to file a report with your local police department

What To Do Next

- Take a deep breath and begin to repair the damage.
  - Close new accounts opened in your name
  - Remove bogus charges from your accounts
  - Correct your credit report
  - Consider adding an extended fraud alert or credit freeze.

Other Possible Steps

- Depending on your situation, you might need to take additional steps
  - Report a misused Social Security number
  - Stop debt collectors from trying to collect debts you don't owe
  - Replace government-issued IDs
  - Clear your name of criminal charges

Kinds of Malware

- Virus
- Trojan
- Worm
- Bot
- Ransomware
- Key Logger
- … and more

Common Sources of Malware

- Porn sites
- Social Media
  - Clicking on links to advertising
- Email attachments and links
  - Be sure you don’t click on an “.exe” or “.com” or “.zip”
  - Be careful of hyperlinks
- Booting from unknown CDs & USB sticks
- Bluetooth transfers
  - Know your source
- Pirated or cracked software (stuff you didn’t buy)

STOP. THINK. CONNECT.

- The first step is to take safety measures, think about the consequences of your actions and connect knowing you have taken steps to safeguard yourself when online.

Virus

- A **computer virus** is a type of malicious software that, when executed, replicates itself by modifying other computer programs and inserting its own code. When this replication succeeds, the affected areas are then said to be "infected" with a computer virus.

From Wikipedia, the free encyclopedia

Trojan

- In computing, a **Trojan** is any malware which misleads users of its true intent
- A user is duped into executing an e-mail attachment disguised to appear not suspicious, (e.g., a routine form to be filled in), or by clicking on some fake advertisement on social media, …
- Payload can be anything e.g. allow an attacker to access users' personal information such as banking information, passwords, or personal identity. It can also delete a user's files or infect other devices connected to the network. Ransomware attacks are often carried out using a Trojan

From Wikipedia, the free encyclopedia

Worm

- A **computer worm** is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself
- Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.
- Many worms are designed only to spread, and do not attempt to change the systems they pass through. However, as the Morris worm and Mydoom showed, even these "payload-free" worms can cause major disruption by increasing network traffic and other unintended effects.

Bot

- A malicious **bot** is self-propagating malware designed to infect a host and connect back to a central server or servers that act as a command and control (C&C) center for an entire network of compromised devices, or "**botnet.**"

Ransomware

- Ransomware is a type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system in a way that is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called *cryptoviral extortion*, which encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them

Keylogger

- A keystroke logger, or keylogger, records every keystroke entry made on a computer
- Capturing sensitive information like usernames, passwords, answers to security questions, and financial information.

Macs Are Not More Secure

- There are fewer malware programs that are targeting Mac OS X – versus Windows
- The rising popularity of Mac operating systems in recent years has made them a prime target for cybercriminals
- Estimates suggest that 700,000 Mac OS X users suffered from the Flashback Trojan virus
- Both OSes are adequately secure when operated with their default security settings along with their vendor’s best practice recommendations
- Mac users are victims of cybercrime just as frequently as PC users.

Take Aways

- ✓Use good PASSWORDS and don’t reuse them
- ✓FREEZE your credit at each of the 3 credit bureaus
- ✓If it seem to be too good to be true, it probably IS
- ✓Protect your devices
- ✓If in doubt – ask a FRIEND