

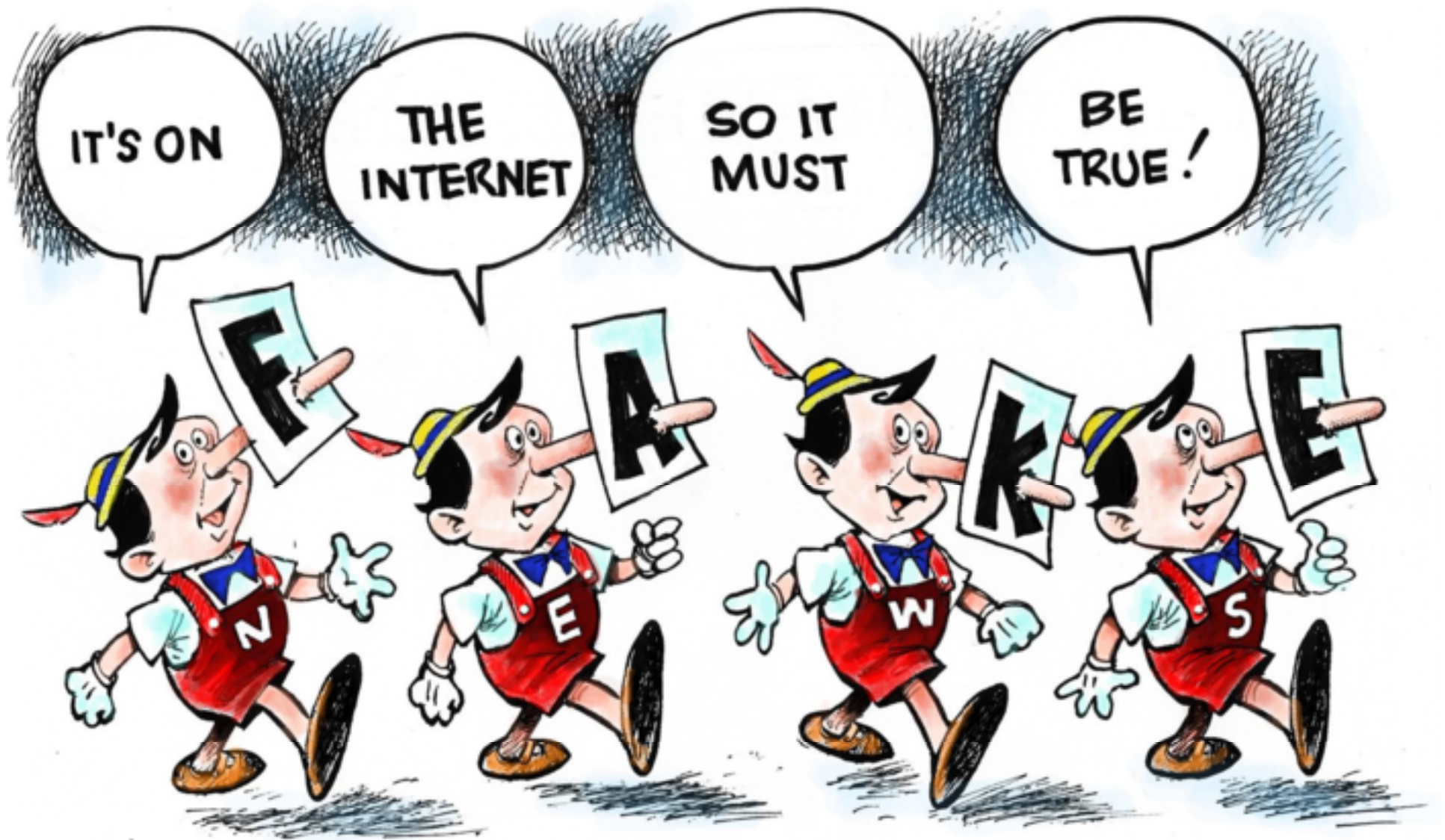
CyberGuardian:

A SecureTheVillage™ Course for Residents



Steve Krantz

IBM Distinguished Engineer, Retired
Ph.D., Computer Science



Course Topics

First Hour:

- Topic 1 – Getting Started
- Topic 2 – Technology Basics
- Topic 3 – Passwords
- Topic 4 - Web Browsing

Second Hour:

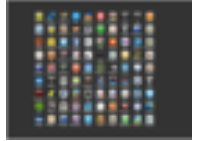
- **Topic 5 – Apps, Social Media, Email & Texting**
- **Topic 6 – Gaming, Parenting, Working from Home**
- **Topic 7 - Personal Computers**
- **Topic 8 - Smart Phones & Smart Homes**
- **Topic 9 – Finances & Files**



CyberGuardian: A SecureTheVillage™ Course for Residents

Topic 5 - Apps, Social Media, Email & Texting





Protection: Apps

- **Installing Apps:**
 - Stick to either Apple's App Store or Google Play for ANY app installation.
 - Both app repositories have reported incidences of scam apps, so be careful
- **Using Apps:**
 - Minimize or Avoid Location & Contact Sharing unless mandatory
 - Avoid entering contests & surveys
- **Removing Apps:**
 - Remove Personal Data FIRST!
 - Follow smartphone instructions for removal

Protection: Social Media

- **Limit your circles** of communication to family, friends & colleagues; ignore unknown “friend requests”;
- **Establish accounts** for major social media apps before a scammer does it for you.
- Even with these limits, **assume everything you post is public**, so be careful...
 - Personal information could be used by hackers
- Review **Security & Privacy** controls on the apps you use (Facebook, LinkedIn, Twitter, ...).
- Take care with passwords and **use 2FA** for all social media sites you use.

The Ten Most Popular Phishing Subject Lines

1. SharePoint: Approaching SharePoint Site Storage Limit
2. Microsoft: Anderson Hauck has shared a Whiteboard with you
3. Office 365: Medium-severity alert: Unusual volume of file deletion
4. FedEx: Correct address needed for your package delivery on ...
5. USPS: Your digital receipt is ready
6. Twitter: Your Twitter account has been locked
7. Google: Please Complete the Required Steps
8. Cash App: Your Account Has Been Closed
9. Coinbase: Important Please Resolve Error Now
10. Would you mind taking a look at this invoice?

(Source: <https://www.techrepublic.com/article/these-subject-lines-are-the-most-clicked-for-phishing>)



Protection: Email & Phishing

- **Use your email program's options to Block and Report SPAM.**
 - Offered in Gmail, Outlook, etc.
- **NEVER open an attachment that you don't COMPLETELY trust!!!!**
- **NEVER click on a link unless sure of the source:**
 - Hover mouse over link (not clicking) to examine URL closely.
 - If unsure, go directly to website from a **bookmarked** link, then login and seek customer service.



Protection: Email

- **Use email aliases** for important social media & financial accounts.
 - Reduces potential for phishing attacks.
- **Avoid sending personal information** via email.
 - Do an **annual email purge** to eliminate any residual personal information.
- If email is **important, upgrade to business service** for better support at a nominal cost.



Protection: Texting & Smishing

- **Texting is useful, but risky (mostly unencrypted)**
 - SMS on Android or iPhone (green background)
 - Select Settings -> Messages -> iMessage for iPhone to get encryption (blue background); takes 2 to tango though!
 - ***Avoid sending private information via text!***
- ***Smishing is Phishing While Texting***
 - To be smished is to receive a *text* from a scammer just as one would receive a phishing email.
 - One click on a link in a smish could infect your smartphone – **don't click on links or images.**
 - Forward to 7726 to report them!

Topic Quiz!

21	I should avoid entering online contests and surveys. T or F?	T
22	I can trust my social media accounts to keep my personal information private. T or F?	F
23	I should establish accounts at major, social media apps to protect my identity. T or F?	T

Topic Quiz!

24	I should NEVER click on attachments or links in my email unless I am SURE of the source. T or F?	T
25	Personal email address aliases are useful for: a. each of my online accounts; b. all financial accounts; c. all social media accounts; d. never.	b, c
26	When should I send important personal information in email? a. Never; b. Only to trusted family; c. Only to trusted companies; d. Always	a

Topic Quiz!

27	If email is important, upgrade to business service for nominal cost. T or F?	T
28	How often should I reduce my stored emails? a. never; b. quarterly; c. monthly; d. annually	d
29	It's ok to send personal information in texts to my trusted friends. T or F?	F
30	If smished, forward the message to 7726 to report it. T or F?	T



CyberGuardian: A SecureTheVillage™ Course for Residents

Topic 6 – Gaming, Parenting, & Working from Home





Protection: Gaming

- Gamers have the same security issues and concerns as everyone else, when not playing.
- Gameplay – civilized behavior rules may not apply
 - Hackers will steal virtual goods
- Game environments riskier than the non-gaming online world - faster pace development, hence more bugs to exploit.
- **Gamers should document any experience of suspecting hacking while gaming, e.g. take a screenshot (use the “print screen” button on the keyboard) and report it to game developers.**



Protection: Parenting 101

- **Parents should be aware and involved**
 - Set rules; teach
- **Share space** where online activities occur
 - Share devices if able
- **Monitor usage** including cyberbullying (incoming and outgoing) – websites, apps, social media
- **Maintain contact** at all times
 - “*RespondASAP*” app (Android only now)
COMPELS a response
- Use **Parental Control Software** – Windows, iOS include as standard



Protection: Parenting 102

- **Children have a legal and financial footprint in the world from birth.**
 - If they have a credit report, freeze their credit.
 - Guard their Social Security Numbers
 - When ready, educate about the measures you have taken.
 - Protect their FAFSA account.

(Source: Cyber Smart, Bart R. McDonough, Wiley, 2019).



Working from Home 101

- **Read the book!** Becoming a CyberGuardian serves your employer's and your personal interests !
- Use your employer's laptop and/or smartphone with **VPN service** to connect to the employer's network
- All **software up-to-date** ; e.g. antivirus, firewalls, device encryption.
- Follow **recommended password/2FA practices**
- Ensure that your **modem/router setup is secure** and this is approved by your company (if they haven't provided this for you)



Working from Home 102

- Ensure that your employer could maintain resource access in the event of your absence.
- Ensure that remote (e.g. cloud-based) storage has been set up to backup your digital work-product.
- Reach out to your work-at-home peers to share do's and don'ts.
- Turn off your smart speaker (e.g. Alexa) if you have confidential work-related teleconferences.

Topic Quiz!

31	Gamers should document suspected hacking and report it to developers. T or F?	T
32	If your young children are online, you should: a. trust them; b. buy them their own computer; c. watch more TV; d. Get involved	d
33	Use your employer's VPN when working remotely. T or F?	T



CyberGuardian: A SecureTheVillage™ Course for Residents

Topic 7 - Personal Computers



Protection: Computer Software



- **Software** must be **up to date**:
 - Use **Automatic Software Updates** for your PC or MAC (or smartphone too!).
 - Vulnerability in old apps or operating system can be exploited by hackers.
 - This includes **ANTIVIRUS!!**
 - This means **ALWAYS!!**

Protection: Computer Loss



- **Protect Physical Access:**
 - Ensure that all users on your computer have strong **passwords** that are difficult to discover. See “Passwords 101”!!
 - Set your computer to **lock** after short time of inactivity (**30 minutes**), and actively lock your computer whenever leaving it.
 - If **stolen**, thieves can mine personal data, so:
 - To possibly recover, install *Prey*
 - <https://preyproject.com/>



Protection: Personal Computer

- **Security/Privacy “suites” standard with typical computer**
 - Windows includes access control, antivirus, firewall, backup, parental control and tune-up.
 - macOS includes access control, backup, firewall, location control,.....
- Several commercial offerings compete: Norton, McAfee, Bitdefender
 - *Generally superior to “pre-installed” offerings*
 - Some commercial suites include additional functions: Password Manager, VPN,

Protection: Computer Files



- **Encrypt all of your computer's disks (storage).**
 - Use FileVault (for macOS) or BitLocker (for Windows).
 - Fixed disks ("C:") and flash drives ("E:")
 - Attackers will need password to access your drive(s) if encrypted.
- **Flash drives are vulnerable:** easy to steal!!
 - Only keep the minimum amount of data on flash drive and wipe it often.

Protection: Computer Disposal



How do I securely **dispose of my old computer**?

- First, transfer all needed files to your new computer
 - Do a direct transfer from old to new (get professional help if needed)
 - Complete backup, e.g. Carbonite: Use to restore on new computer
- Second, erase ALL contents on your old computer's hard disk
 - Several free tools available: most recommended is <https://dban.org/>
- Third, donate (or bequeath to your children!)

Topic Quiz!

34	When should I update my device software? a. Always; b. Tuesdays; c. Annually; d. Monthly	a
35	Antivirus is optional on today's smart devices. T or F?	F
36	My smart devices are set to lock up after ____ of inactivity. a. One day; b. 30 minutes; c. Never; d. 1 minute	b

Topic Quiz!

37	Encrypt your files on all devices. T or F?	T
38	It is unnecessary to erase my old files on my old device after migrating. T or F?	F



CyberGuardian: A SecureTheVillage™ Course for Residents

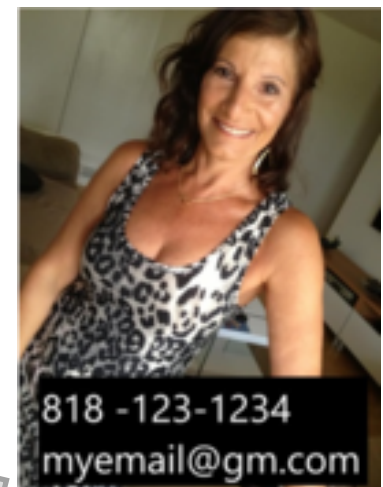
Topic 8 – Smart Phones & Smart Homes



Protection: Phone Access (1)



- **Device Security**
 - **iPhone** - Use *Touch ID* (or Face ID) and memorable, non-obvious pass code (4 or 6 digits) for access.
 - **Android** – Use *fingerprint or facial recognition* by *Settings -> Lock screen and security -> Fingerprint scanner* or Facial Recognition
 - **Lock Screen** – make it better by taking photo and editing in email and alternate phone #.





Protection: Phone Access (2)

- **Device Security (continued)**
 - **Set a PIN Access Code with Phone Company!**
 - Defeat “SIM Swap” Attack:
 - Scammer with your phone # calls your provider and requests new SIM!

Protection: Phone Recovery



- **Recover Lost or Stolen Phone?**
 - Only if “on” and not “reset”, so unlikely but worth a shot!
 - iPhone – icloud.com/find
 - Android – android.com/find or *Prey* app



Protection: Phone Privacy

- **Apps Settings for Privacy:**
 - **Limit “Location Sharing”** - only when necessary (iPhone: Settings, Privacy, Location Services, Share My Location..),
 - Even without sharing, cell phone can be tracked through cell towers and/or Wi-Fi networks.
 - **Limit Contacts Access** by apps to reduce risk of uncontrolled sharing.



Protection: Scams/Robocalls

- **Incoming Call (and Text) Control**
 - Add **known persons to Contacts** asap.
 - Then **IGNORE** all other calls and texts.
 - Especially “Unknown”, “No Caller ID”
 - Google Pixel phone can be set to block known spam #s
 - Verizon offers free “Call Filter” app to identify spam/robo calls. “Filter Plus” service for \$3/mo.
 - T-Mobile, AT&T, Sprint also offer call blocking.



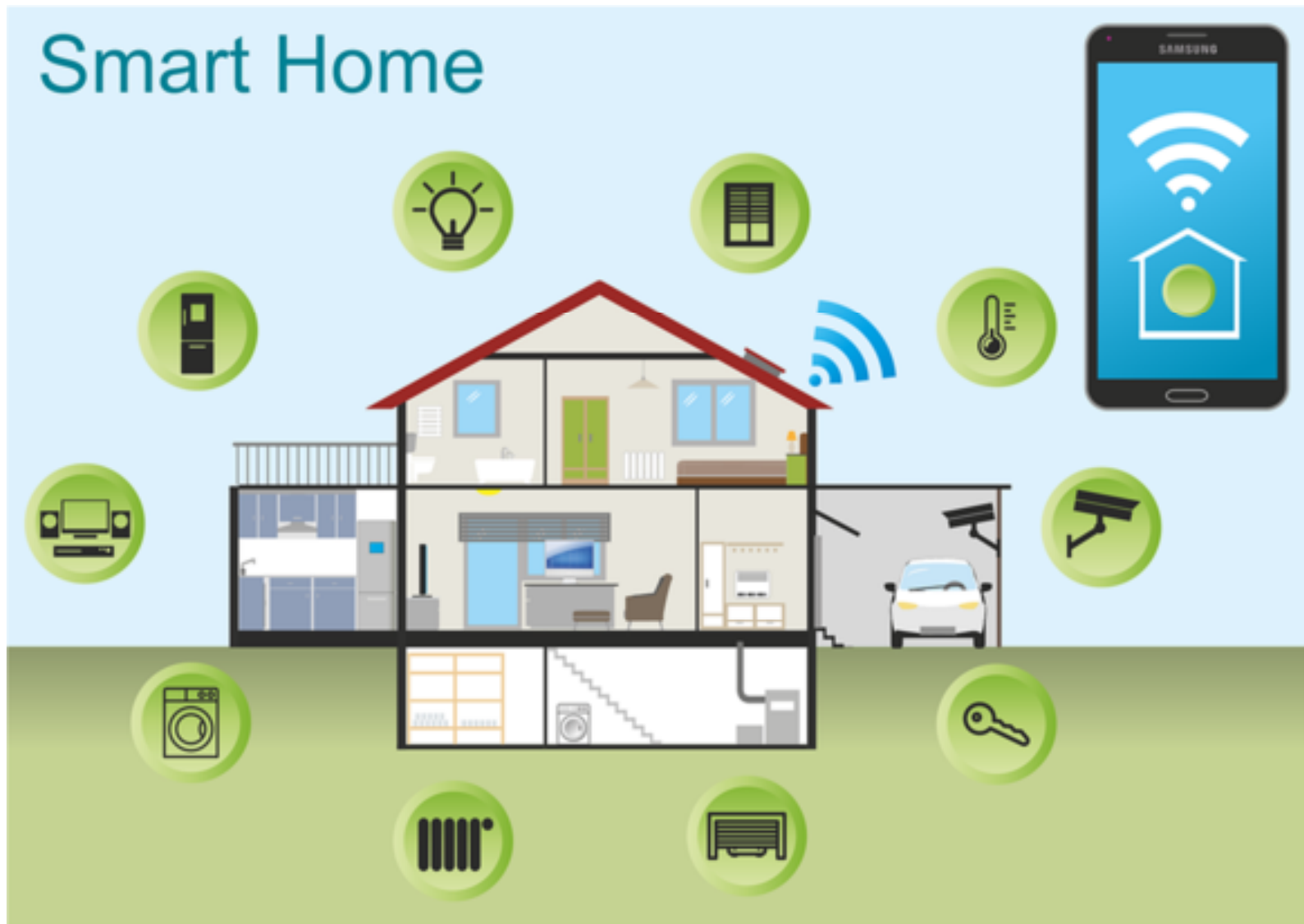
Protection: Phone Migration

How do I **securely** migrate from an old phone to a new one?

1. Seek an in-store data migration from old to new phone.
 - Or for DIY, (1) backup all phone data to the cloud, (2) setup new phone and (3) re-access cloud data.
2. Second, delete all information on any SD or SIM cards from old phone and remove them or install in new phone.
3. Do a factory reset on old phone.
4. Recycle or donate (your children won't want your old phone!).



Smart Homes





Smart Homes

Personal Examples:

- Heating/Cooling – Nest Thermostat + Smartphone
- Security – Ooma-Box + Motion Sensor + Door Sensor + Water Sensor + Smartphone
- Smart TV – Samsung + Wi-Fi + Netflix
 - Unwanted tracking!
- Travel Reservations – Alexa + Wi-Fi + Airline
 - Scam website intrusion!

Risk:

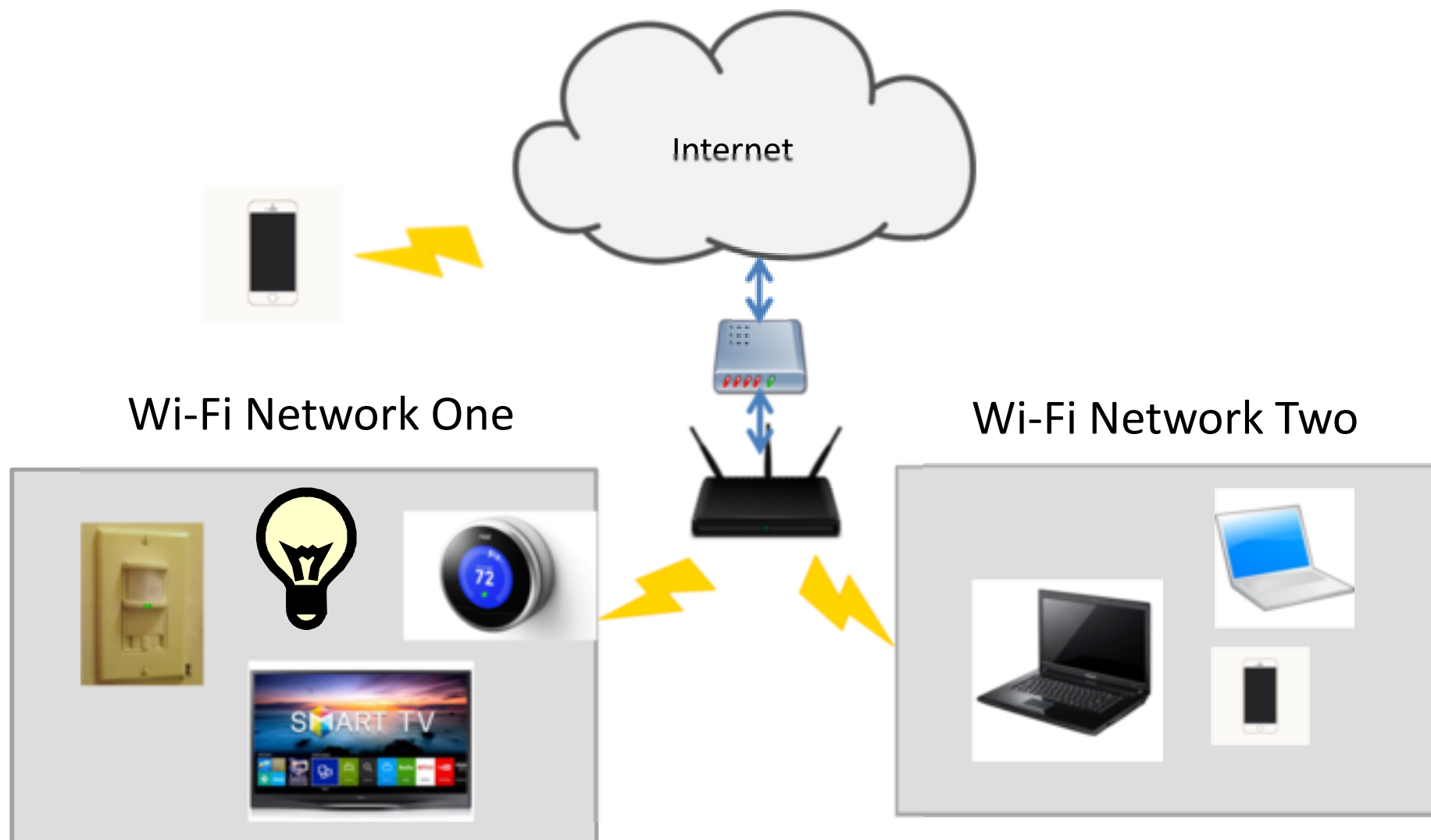
- Personal data “leakage” to scammers, thieves

Protection:

- Separate home Wi-Fi network for smart devices

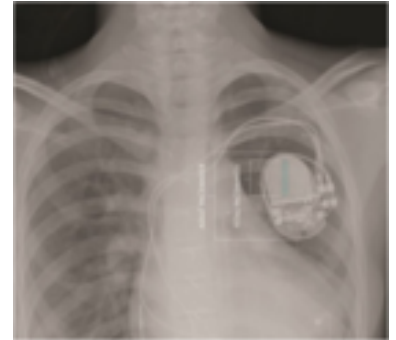


Smart Homes



Smart Body, Hacked?

- Increasing numbers of implantable medical devices are now gaining internet connectivity,
- Doctors can monitor remotely, and even update the devices to tweak a treatment plan.
- Hackers could hijack that hardware, and make changes to the way the devices work.
- No attacks have been successful, proof-of-concept attacks have been available for years.
- <https://www.nytimes.com/2008/03/12/business/12heart-web.html>



Topic Quiz!

39	<p>How can I securely, maximize my chances of getting a lost smartphone returned?</p> <ul style="list-style-type: none">a. Edit my lockscreen image with my email address and a friend's phone number;b. Install Find My iPhone app;c. Find My Device feature on Androids;d. Pray loudly	a, b, c
40	<p>How do I protect my device from unauthorized use?</p> <ul style="list-style-type: none">a. Set up a non-obvious pass code;b. Use touch/facial recognition;c. Set up a simple, memorable pass code;d. Do nothing	a, b

Topic Quiz!

41	Only set up location sharing on your device for apps that require it. T or F?	T
42	Always authorize contact sharing when requested by apps on your smartphone. T or F?	F

Topic Quiz!

43	Set up a pin access code with your phone service provider ASAP. T or F?	T
44	What should I do to minimize or prevent robo calls? a. Ignore callers that are not in your Contacts; b. Pick up all calls, curse and hang up; c. Contact phone service providers for blocking service; d. Pick up all calls, threaten to sue and wait for a response.	a, c
45	It's unnecessary to erase all files from old phone when migrating to a new phone. T or F?	F

Topic Quiz!

46	Don't use your voice assistant to find numbers for important calls. T or F?	T
47	How should I set up my smart home network? a. Keep the original - no changes needed; b. Put all IoT devices on a separate (guest) network; c. Each device should be on a separate network	b



CyberGuardian: A SecureTheVillage™ Course for Residents

Topic 9 – Finances & Files





Protection: Credit

- **Freeze Your Credit** (it's free and very important)
 - Equifax, Transunion, Experian, Innovis offer online freeze requests – each sends PIN #
 - Selectively unfreeze for new credit needs; refreeze – also free.
 - Freeze doesn't impact prior, current creditors
- **Get free, annual credit reports** at AnnualCreditReport.com
- **File your taxes early** to foil identity thieves.
 - **Get an IRS IP Pin** to prevent scammer submitting your taxes.



Protection: Finances

- **Protect Your Financial Transactions**
 - **Frequently Monitor Your Financial Accounts**
 - Consider Quicken
 - **Dedicate a single device** to all financial activities (e.g. home computer)
 - **Set up account alerts** for credit/debit cards.



Protection: Identity

- **Consider identity-theft insurance, but read the fine print.**
 - Basic insurance covers only the costs of remediating your identity, not the losses.
 - Per Consumer Reports , it's a waste of money. Less than 1% of the victims suffer any serious loss per their research.
 - **Freezing your credit files mitigates the need for this significantly.**



Protection: Payments

- **Online payments**
 - Credit, Debit Cards or Checking Acct
 - Only with an **https** website (encrypted transfer)
 - Paypal – encrypted for transaction privacy, so secure
- **In-Store (Mobile) payments** – Place phone near store checkout reader
 - Debit/credit card connected to “wallet” phone app (Apple Pay w/Wallet app or Samsung Pay or Google Pay)
 - Near *field communication* (NFC) makes payments between device and retailer’s check-out reader.
 - ***Safer, faster and easier than paying cash or using a card***

Protection: File Storage



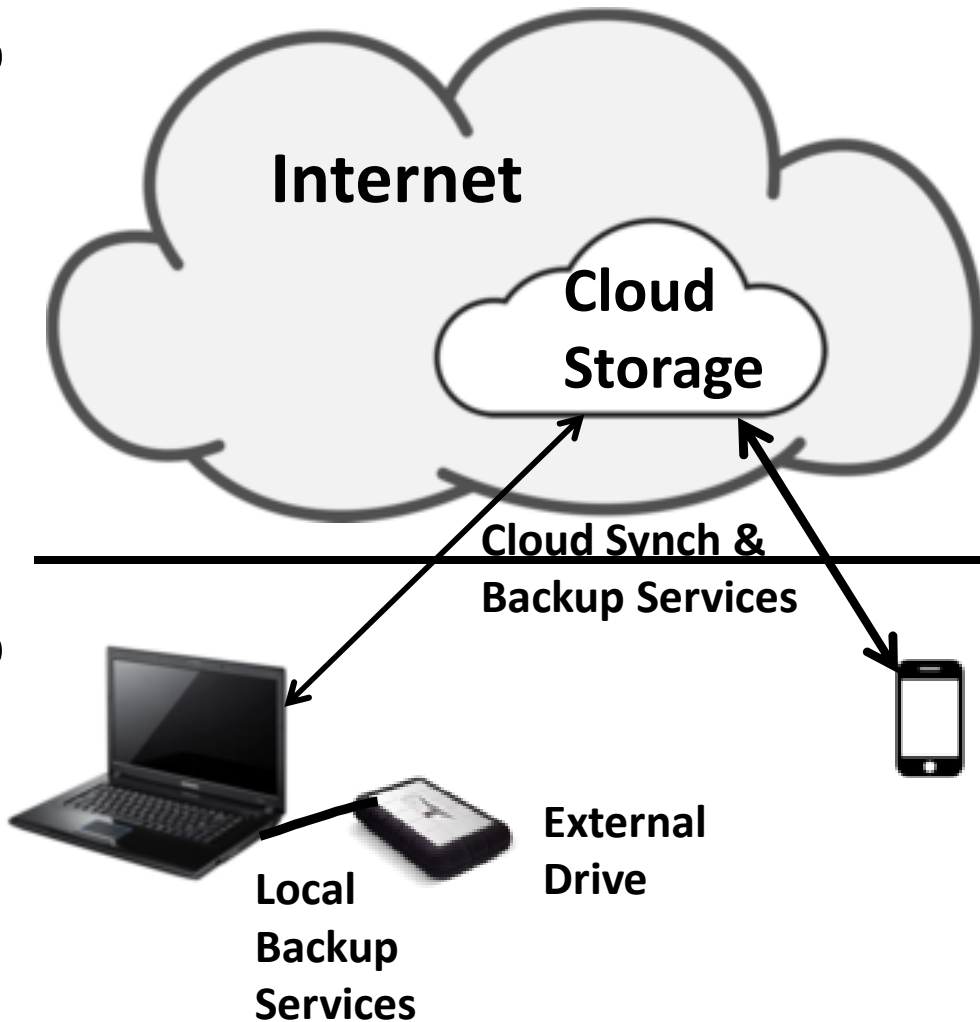
- **What to Keep and How Long to Keep It?**
 - Email –consider annual purge to minimize risk
 - Browser History & Cookies - clear at least annually (regularly if bugged by ads)
 - In Chrome: History -> History -> Clear Browsing Data
 - In Safari Mobile: Settings -> Safari -> Clear History and Website Data
 - Legal, Financial , Business– 3 years minimum
 - Photos, Videos, Music – forever

File Storage Alternatives



Remote Storage

Local Storage



- **Remote or Cloud Storage**
– files copied over the Internet from your laptop/computer or smartphone to a server by Cloud Synch or Backup Services.
- **Local Storage** – the files on your laptop/computer and smartphone or on an external drive connected to your laptop/computer, copied by Local Backup Services.

Protection: Backup



- **Backup/Recovery** of Files – mitigates device theft, loss, failure, ransomware, overflow
- Alternatives:
 - No backup – risky!
 - Local backup – inexpensive external disk.
 - Mac offers “Time Machine”
 - Windows 10 offers “Backup using File History”
 - ***Remote backup – best for disasters...***
 - Carbonite is my app, Cloud solutions are alternatives
- Overflow?
 - Periodically delete or use the Cloud
 - Cloud allows device sharing

Protection: Kick the Bucket



The Traditional:

- Wills, Trusts, Durable Power of Attorney, Advanced Health Care Directive
 - Online Tools: Quicken Willmaker & Trust 2020
- Life Ins. Policies
- Burial/Funeral Instructions
- Safe Deposit Box Keys/Access for Original Documents

+ Kick the Bucket Letter (next slide)

Protection: Kick the Bucket



“Kick the Bucket” Letter to Heirs

- Computer(s) and Smartphone(s) Access instructions
- Critical File access: Backup files, disks and Cloud accounts
 - Tax documents, such as TurboTax files
- Online Accounts IDs/Passwords/Pins
 - Password Mgr, Life Insurance, Investments, Banks (Checking/ Savings/Credit Card), Mortgages, Loans, Medicare,
- ***Place Copies in Safe Deposit Box and Safe Place in Home AND.....***

Protection: Almost Kick the Bucket



Emergency Key Document Storage

- Docubank.com – online store for advance directives, lists of doctors, medications, HIPAA release forms.
 - ***Wallet card for emergencies***
- Everplans.com – a “digital file cabinet” for medical directives, funeral preferences, insurance, deeds, etc.
 - Deputy assignment
 - Source: NY Times, Mar 27, 2020, “Making a Will (or Updating One) Just Became More Complex

Topic Quiz!

48	How can I best protect my identity and credit? a. Pray frequently at your house of worship; b. Freeze your credit at the 4 credit bureaus; c. Check your credit annually at each of the 4 credit bureaus; d. Use cash only	b, c
49	Frequently monitor financial accounts and set up automatic alerts. T or F?	T

Topic Quiz!

50	<p>How should I protect myself from someone filing taxes in my name?</p> <ul style="list-style-type: none">a. File my taxes early;b. Get an IP Pin from the IRS;c. Make regular estimated tax payments throughout the yeard. Become famous	a, b
51	<p>What is the most secure way to pay at the grocery store?</p> <ul style="list-style-type: none">a. Use cash;b. use a debit card;c. use a credit card;d. use smartphone Pay apps	d

Topic Quiz!

52	How often should I purge unnecessary files on my devices? a. Yearly; b. Never; c. Monthly; d. Whenever	a
53	What is the best way to backup my personal computer and smartphone files? a. local external drive; b. cloud synch of important files; c. continuous remote backup of all files	C

Topic Quiz!

54	How should I communicate my personal online details to my heirs? <ul style="list-style-type: none">a. Verbally;b. Detailed letter stored in at least 2 secure places;c. They don't care;	b
----	---	---



CyberGuardian: A SecureTheVillage™ Course for Residents

Final Thoughts





Secure is a Relative Term

There is NO “Completely Secure”!!

Area	Most Secure	Mezzo Secure	Least Secure
Website Login	Yubikey	2FA	ID/password
Network	VPN	Home Wi-Fi, Cellular Data	Public Wi-Fi
Password	Spot likes belly rubs on his tummy	Xaztbe\$24!!	“password”

Final Exam (1)!!

1. Which is the most secure password? Stevekrantz, Schmootz11\$, “My dog Spot has fleas on his belly.”
2. Public Wi-Fi (even if password protected) is not always safe for sensitive activities – True or False?
3. What is a smishing attack?
4. Is it safe to share my location with apps on my phone? – True or False?
5. Americans can legally obtain one free credit report yearly from each of the four credit bureaus – True or False?

Final Exam (2)!!

6. Ransomware involves criminals encrypting and holding users' data hostage until paid – True or False?
7. Wi-Fi traffic is encrypted by default on all wireless routers – True or False?
8. https:// in a URL means that information entered into the site is encrypted – True or False?
9. A VPN minimizes the risk of using insecure Wi-Fi networks – True or False?
10. What is two factor authentication (2FA) ?

Protection: Top Ten List

1. Freeze your credit at the 4 credit bureaus and check credit rating annually at each.
2. Set up 2FA at your important online accounts (government, banking, investments, credit cards,..).
3. Set up your home router with a non-personal SSID, memorable and strong password, and WPA2 encryption.
4. Keep software up to date on all devices.
5. Install antivirus on computer and smartphone.

Protection: Top Ten List

6. Long, memorable, unique passwords at all online accounts.
7. In email, don't click on attachments or links unless SURE of source.
8. Maintain a remote backup of computer files.
9. Create a smartphone lock screen with alternate phone number and email.
10. Create *Kick the Bucket* letter for your heirs.

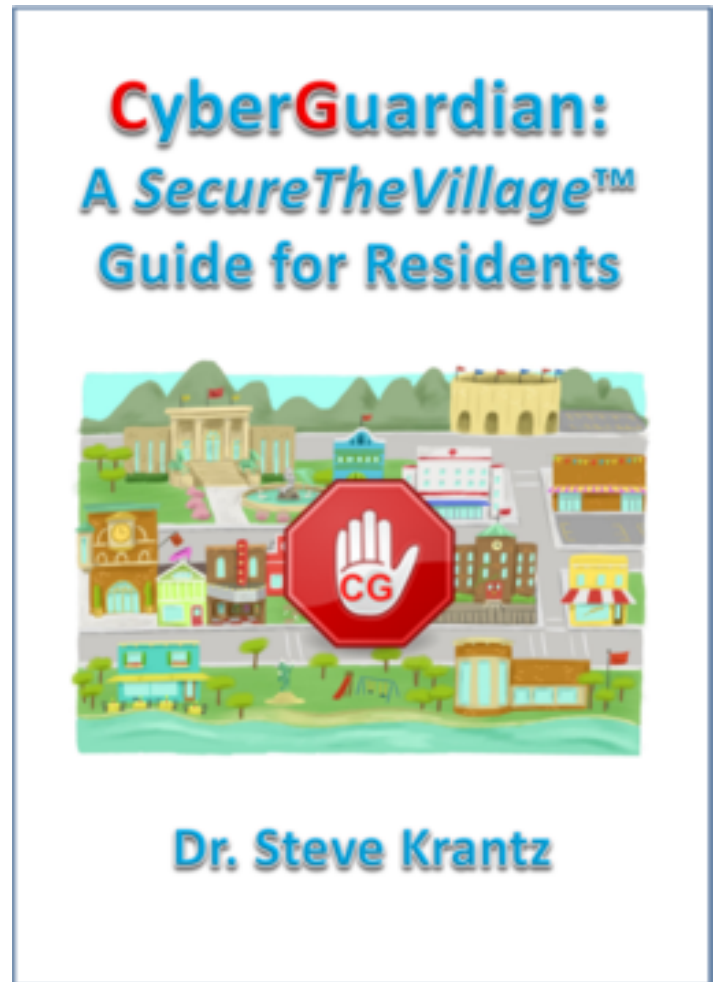
Must Haves: The Six Pins

1. Experian Freeze Pin
2. Transunion Freeze Pin
3. Equifax Freeze Pin
4. Innovis Freeze Pin
5. Cellphone Provider Pin
6. IRS IP Pin (irs.gov)



Security Checklist: 54 Do's & Don'ts

- The heart of my new book on Amazon
- Checklist is available for download at www.nerdsiview.com



Become A CyberGuardian



- Cybercrime is a Reality for Individuals & Businesses
- **Make Yourself Hard to Impersonate (2FA, the Six Pins)**
- **Know with Whom You're Communicating**
 - ***"Distrust and caution are the parents of security."* Benjamin Franklin**
- **Be Prepared (software updated, data backed up, kick-the-bucket letter,)**



6/11/2020

(c) Alan Steven Krantz, 2020



67

Questions?



- Thanks for attending the class!
- **Followup Questions:** stevek@bipedinfo.com
- **Reference: CyberGuardian: A SecureTheVillage Guide for Residents on Amazon.**
 - <https://www.nerdsiview.com>
- **Followup Support: Jeffrey Krantz,**
jeffk@bipedinfo.com, 818-625-2178

Backup





Copyright 2003 by Randy Glasbergen. www.glasbergen.com



“I get to the office around 8:45, pour myself a cup of coffee, turn on my computer, delete all the spam, and then it’s time to go home.”

71



“We forgot to back up our files, so we’re asking everyone to remember everything they’ve typed during the past 10 days.”



I HAVE A
NEW HOBBY.
IT'S CALLED
PHISHING.



www.dilbert.com scottadams@aol.com

I SEND FAKE BANKING
E-MAILS TO GULLIBLE
EXECUTIVES. THEN I
FIND OUT THEIR
FINANCIAL INFOR-
MATION AND USE
IT TO STEAL THE
MONEY THEY DON'T
DESERVE.



8-12-05 © 2005 Scott Adams, Inc./Dist. by UFS, Inc.

8-12-05 © 2005 Scott Adams, Inc./Dist. by UFS, Inc.

Dear Customer,
This is your bank. We forgot your
social security number and password.
Why don't you send them to us so
we can protect your
money.

Sincerely,

I. B. Banker

LOOKS
LEGIT.



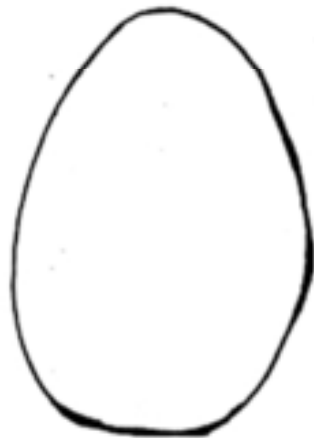


THE INTERNET OF EVERYTHING

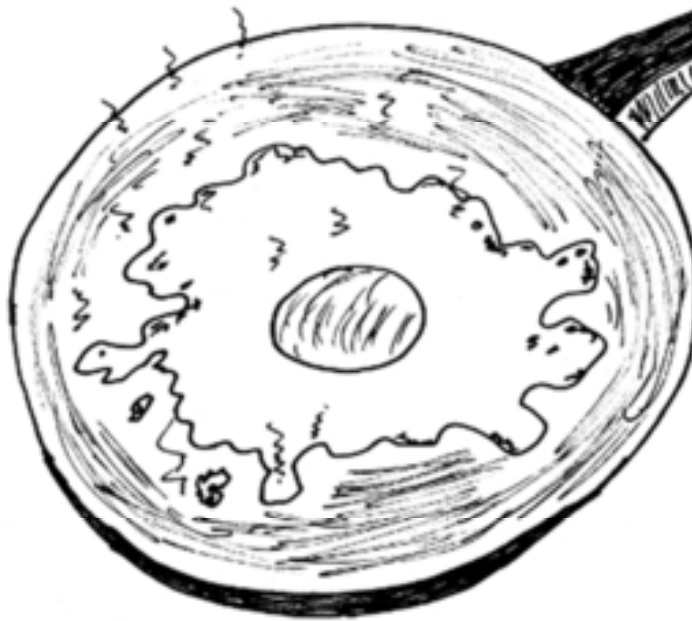
I TOLD YOU TO PICK UP MILK ON THE WAY HOME.
DON'T YOU LISTEN TO
ANYTHING I SAY?!!



THIS IS YOUR
PRIVACY.



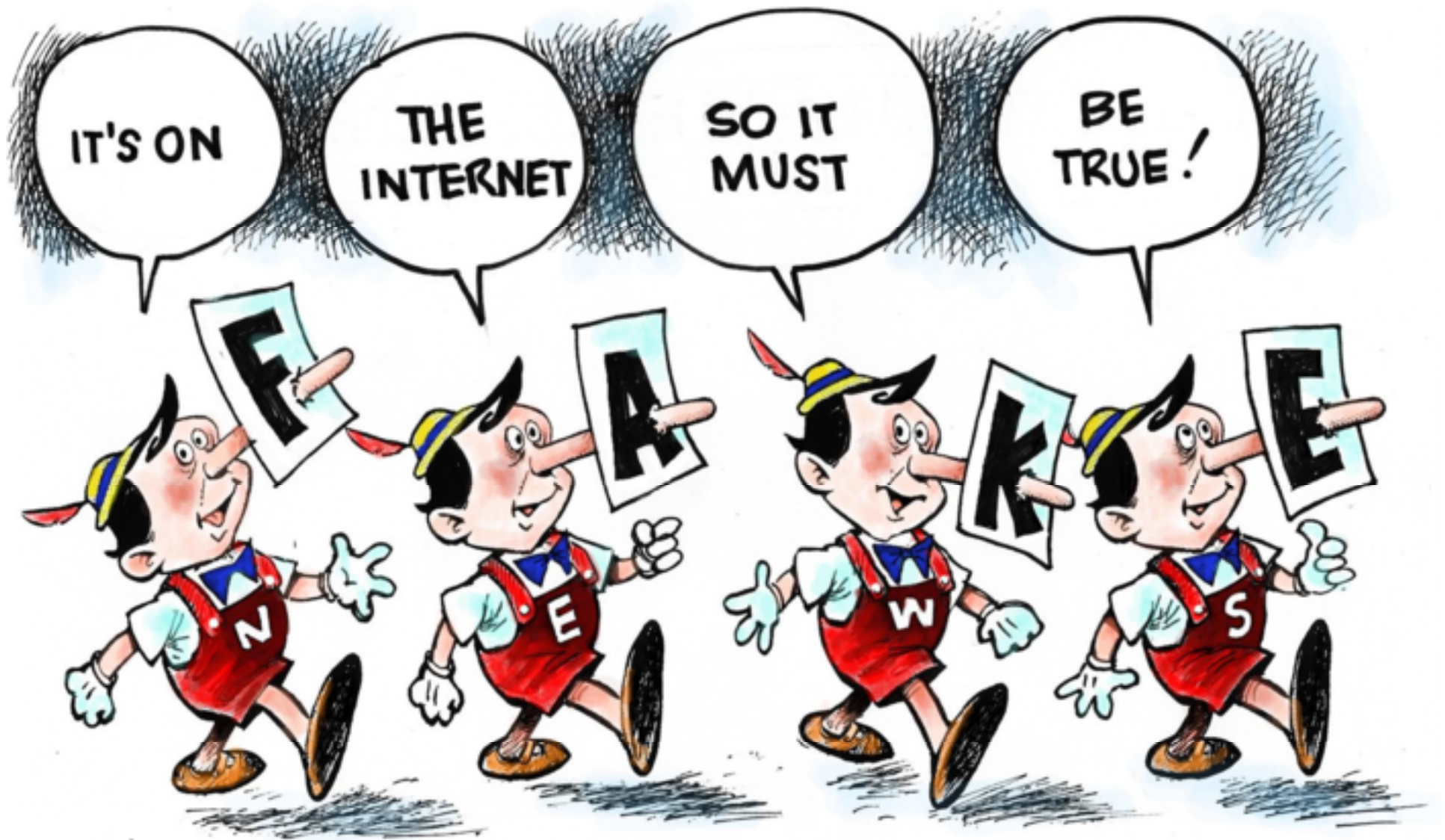
THIS IS YOUR PRIVACY
ONLINE.



ANY QUESTIONS?



" MAYBE WE SHOULD TRY A DIFFERENT
SECURITY APPROACH THIS YEAR. "





"I think we're named after computer passwords."



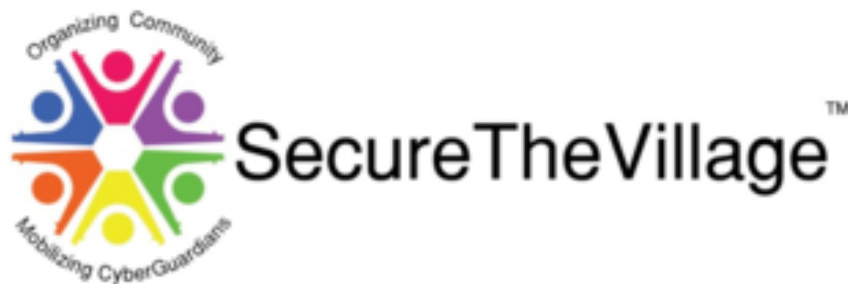
Protection: Passwords 101

What's Your Password?



A Secure The Village **Roundtable Event**

The Mission: a Cybersecure Los Angeles





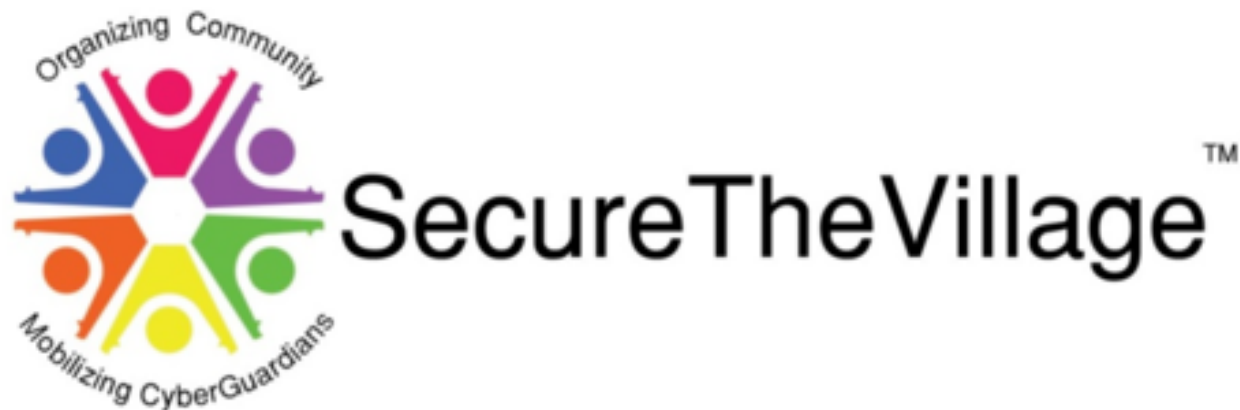
Final Thoughts



- ***It's a dangerous cyber-world out there, be safe!!***
- Cybercrime a Reality for Individuals
- There is Technology Available to Help
- **MOST IMPORTANT: Freezing Credit, 2FA**



Backup

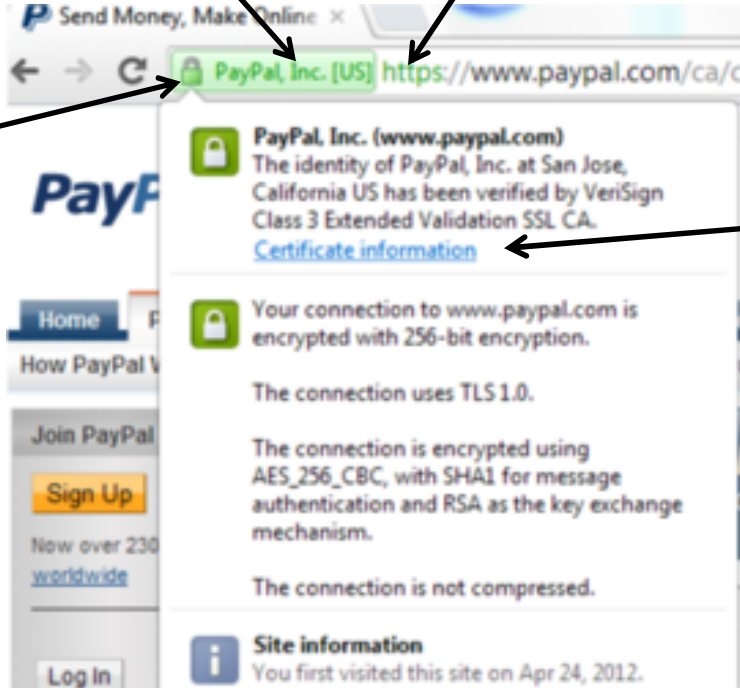


The Mission: a CyberSecure Los Angeles

A Model for Other Communities

Protection: Web Browsing (1)

- Use Browser clues to determine website safety



Owner name implies EV* Certification

Implies encryption

Lock indicates relatively “secure”; when clicked browser provides details.

Check on certificate and who issued to

* Extended Validation

The screenshot shows a browser window with the PayPal website. A security information overlay is visible, showing the site's identity, encryption details, and site information. Annotations with arrows point to specific elements: the site name 'PayPal, Inc. [US]', the lock icon in the address bar, the 'Certificate information' link, and the 'Site information' section.