





Technology is Hard!

- Constantly evolving technology**
 - Creates uncertainty – managing uncertainty is harder.
- Integrating new technologies into a government environment**
 - Competition for time and attention of leaders concerned with a lot of other issues
- Dynamics that work against long-term planning**
 - "We can defer that purchase for another year, can't we?"

Key Technology Management Challenges

- Prioritizing**
Determining what we need, want, can afford
- Identifying**
Understanding that there are more risks than cyber-security
- Accepting**
Knowing that managing technology and their risks is a not race with a finish line; it's a journey
- Defining**
Understanding that "technology" is more than "information technology"

MINIMUM Technological Proficiency

- Leadership**
- Planning**
- Decision-making**
- Budgeting**
- Technical Competency**
- Cyber Hygiene**
- Proficiency**

To the extent one is weaker than the others, they are all weaker.

IN THE NEWS

- TEXAS W-2 SCAM**
Texas city loses 800 city employees W-2s in phishing scam
- NORTH KOREA** tries to make hacking a profit center
- A CYBERATTACK** hobbles Atlanta, and security experts shudder
- OHIO FIRE MESS**
Servers for the district Internet and phones were in the basement of the building which got flooded.
- NJ MAN HACKS UNIV.**
Internet attack that brings down Rutgers
- NJ POLICE DEPT HACK**
Ransomware forces PD to paper and pen

HERE'S THE CYBERSECURITY PROBLEM



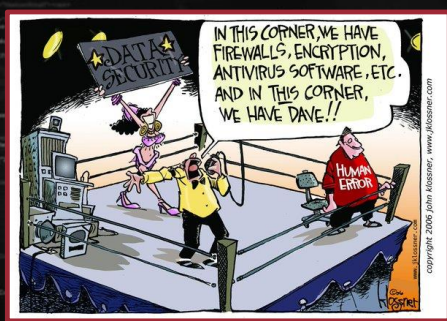
Criminals try to **manipulate** people into divulging **personal** or **business** information or trick them into schemes to defraud



Criminals can be **individuals** or part of industrialized, **cyber** crime businesses




There is **NO SINGLE FIX** The threats keep changing
It's a perpetual battle



HUMAN ERROR
THE WEAKEST LINK

DEFINITIONS

SOCIAL ENGINEERING



The acquisition of special knowledge by means of wit and skill.

- Fraud
- Deceit
- Fear
- Greed


FRAUD

DEFINITIONS

MALWARE

Destructive form of computer software transmitted by email and website links

- Viruses/Trojans/Rootkits/Worms
- Spyware
- Crimeware
- Adware
- Cryptojacking
- Typosquatting




DEFINITIONS

PHISHING

A form of social engineering that appears as email or a text message that attackers use to gain login credentials or account information

And its evil cousin, the targeted Spear-Phish or Vishing, using voice to fool you



Why Criminals Attack

- To steal personal information
- Steal Access Credentials
- Fool you into doing something you would not do - like order stuff or send money
- To control your system:**
 - For access to data and controls
 - As a launching point to attack other systems;
 - Use your processing resources for their gain
- Introduce ransomware via email or network access

PRIME ATTACK AND THREAT VECTORS

TARGETED ATTACKS	MASS ATTACKS	MAN-IN-THE-MIDDLE	UNSECURE HUMANS
<ul style="list-style-type: none">Government agencies are generally targetsIt also happens if something goes wrong and you get negative press attention	<p>This stems from successful email phishing, social engineering, plus "brute force" attacks on networks: affects people and organizations</p>	<p>An email link goes to a log-in page that looks legit, but is fraudulent and will steal your credentials</p>	<ul style="list-style-type: none">Clicking on the wrong link or opening the wrong fileAn employee who steals data for resale or illegal use

WHEN EMAIL TURNS EVIL

MALWARE HIDDEN IN EMAIL

- Fake links entice you to open harmful websites
- Embedded images containing hidden code
- Spofed "from" addresses
- Coupons, "too good to be true" ads
- MS Office or other file attachments containing macros with viruses or malware (.docx, .xlsx, .pptx, .html, .zip)

PHISHING EMAIL EXAMPLES

EMAIL FROM TRUSTED ORGANIZATIONS

01 DELIVERY ALERT Post office UPS FedEX	02 OVERDUE BILL Utility company Credit card	03 TAX RETURN Fake return alert
04 RETAIL RECEIPT Amazon Costco	05 CREDIT CARD REWARDS Fake credit card rewards	06 LOGIN ALERT Company login or password change alert

Each variation relies on our instinct to act on messages that appear to be urgent

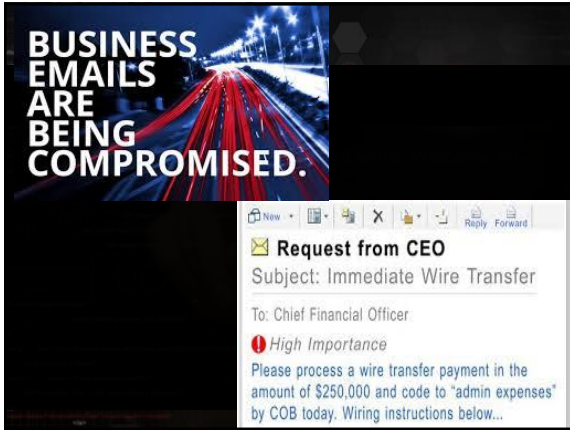


PASSWORD ALERT

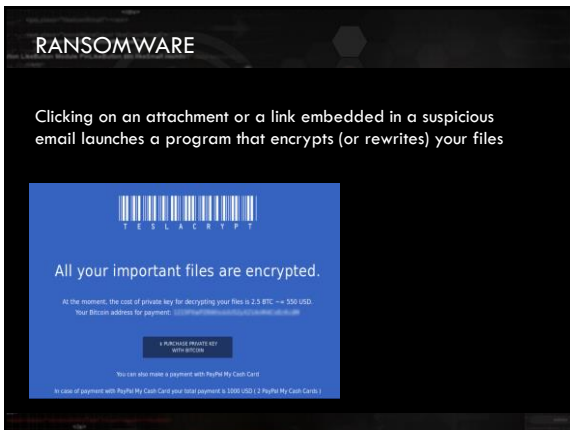
If you receive an email alert like this one from Gmail, you need to change your password immediately.

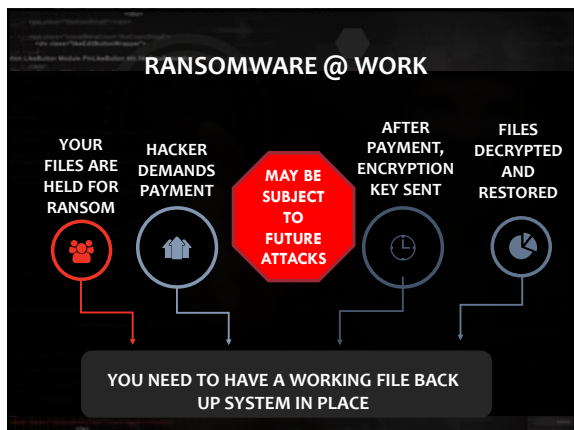
But how?

A screenshot of a Gmail email alert. The subject is "Someone has your password". The email content says: "Hi John, Someone just used your password to try to sign in to your Google Account john.podesta@gmail.com. Details: Saturday, 19 March, 8:34:30 UTC. IP Address: 134.249.139.239. Location: Ukraine. Google stopped this sign-in attempt. You should change your password immediately." There is a "CHANGE PASSWORD" button at the bottom.

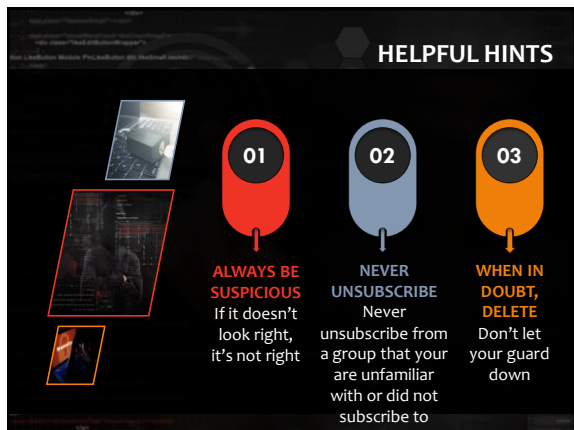






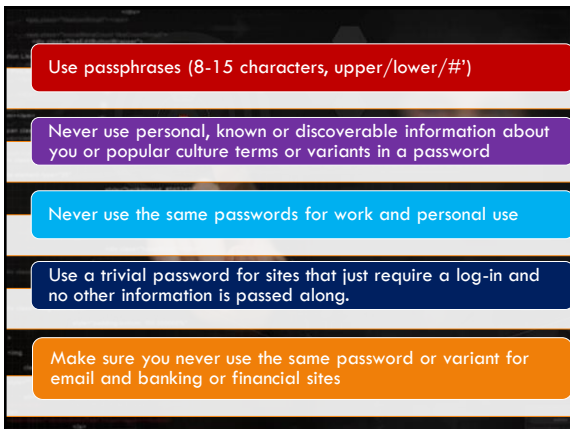




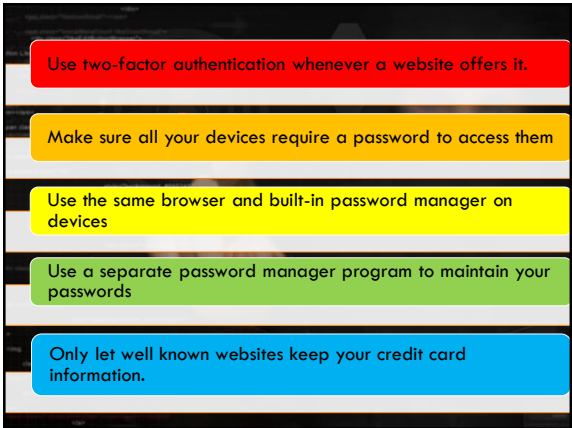


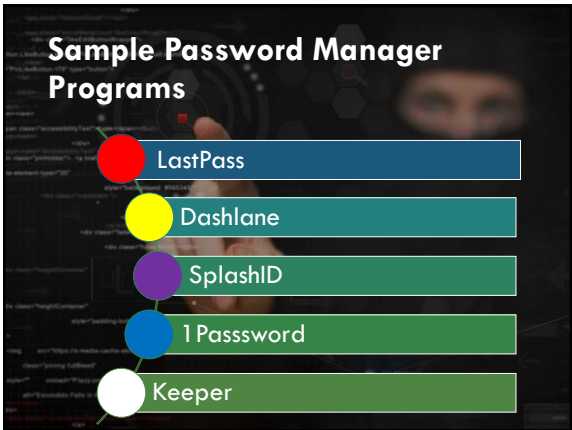


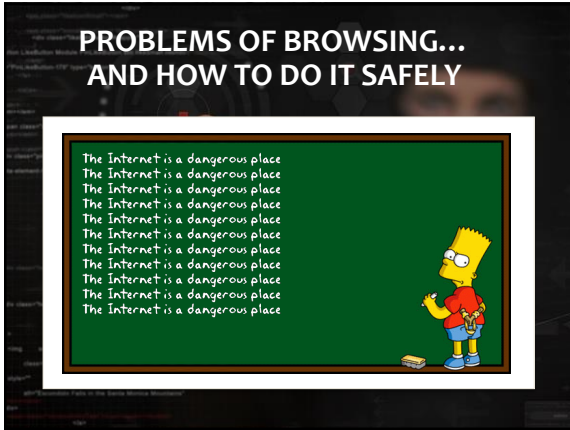


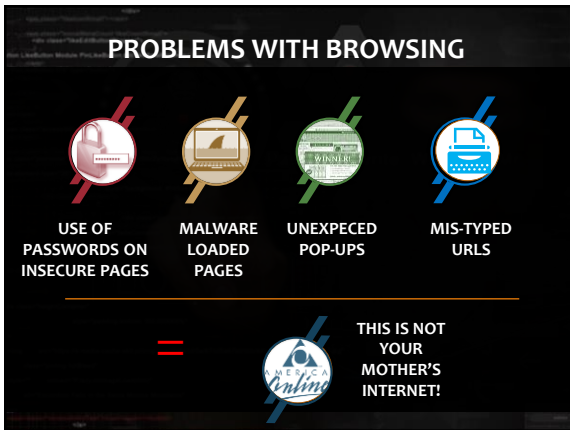



















KNOW IF A WEBSITE IS SECURE!

http://www._____ 

https://www._____ 

“S” = SECURE/ENCRYPTED
No passwords or credit cards on
“non-S” sites

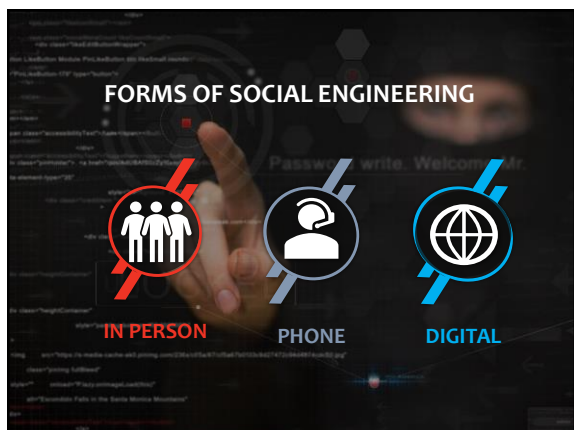
SAFE BROWSING SKILLS

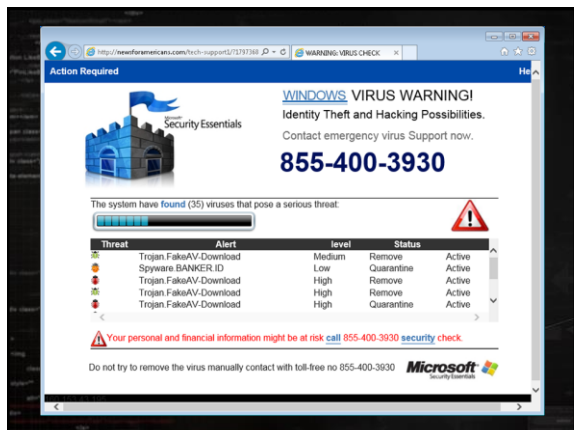
DON'T CLICK ON POP-UPS	WARNING SCREEN APPEARS	WATCH WHERE YOU CLICK	KNOW WEB ACTIVITY IS TRACKED	TEST PAGES: FAKES DON'T RESIZE
01	02	03	04	05
DO NOT CLICK on unexpected pop-ups or messages when browsing - turn off pop-ups in settings	Close or disconnect: at work, unplug from network then call IT; if at home, close the window, unplug, or reboot	Cluttered websites will tempt you with one thing, and fool you into clicking on something else	Web browsing activities are tracked (even if you clear history)!	Look at it full size, then drag corner to shrink it. If it won't or doesn't, close the browser!
				

MORE SAFE BROWSING SKILLS

 IF IT SEEMS TOO GOOD TO BE TRUE, IT IS	 TECH SUPPORT WARNINGS ARE SCAMS	 DON'T DOWNLOAD TOOLBARS OR CLEANERS	 FREE, ISN'T. IF YOU ARE NOT PAYING FOR IT, YOU ARE THE PRODUCT
---	--	--	---







PHONE HOAXES

- PERSONAL INFORMATION**
Callers claiming they are from a vendor or IT asking for confidential information
- TEXT MESSAGE LINKS**
Don't click on links in text messages from unknown senders
- SECURE MOBILE DEVICES**
Always set a passcode on your phone
- CAN YOU HEAR ME?**
Scammers record you saying "YES" then they claim you agreed to something else
- DON'T TRUST CALLER ID**
Caller ID can be spoofed. Always verify identity
- TECH SUPPORT WILL NOT...**
...call you tell you your system has a problem. Just hang up.

USB SECURITY

48% OF PEOPLE WHO FIND A USB STICK IN A PARKING LOT WILL PLUG IT IN

- DROPPING USB STICKS IS EFFECTIVE
- PEOPLE PLUG IN USB DRIVES QUICKLY

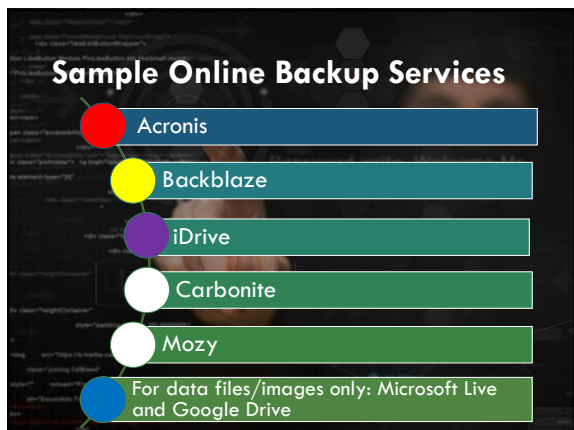
AT-HOME BACKUP CHALLENGE

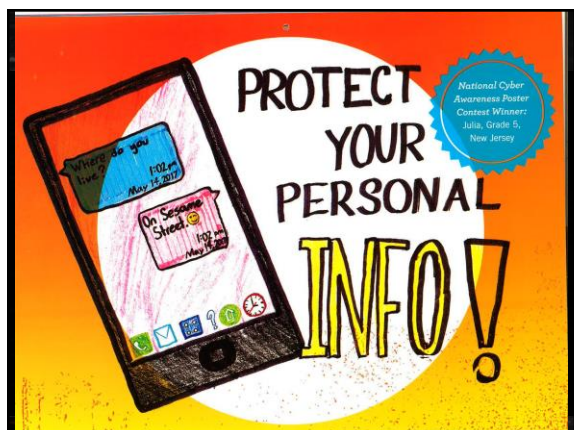
You need to backup because bad things can happen

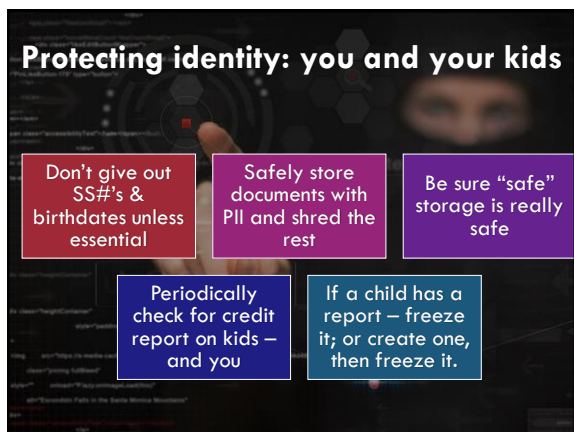
You need a plan based on what you store locally and what you keep in the cloud; and your skills.

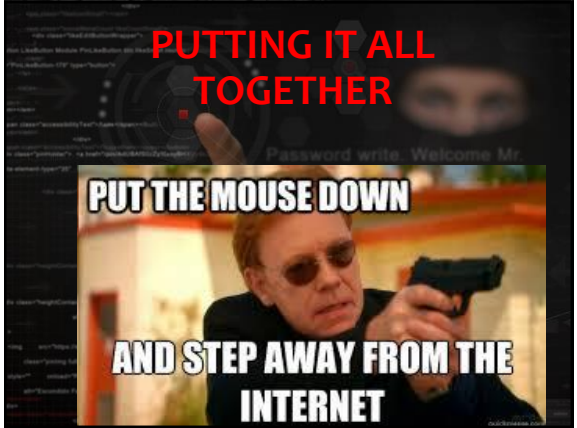
Backup your operating system and data files automatically

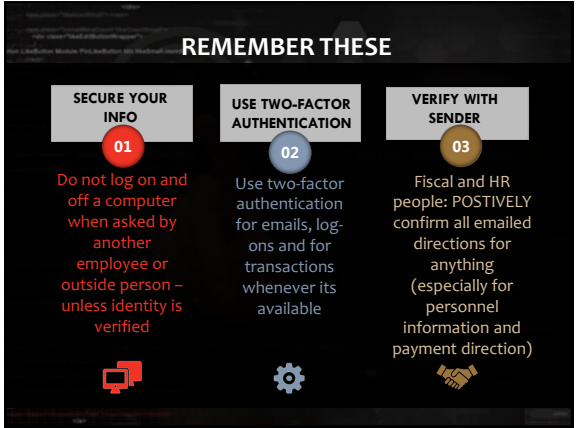
- Cloud backup backs up files constantly, and can do system back-ups
- Local storage needs an external drive and good software, plus online (cloud) service
- Phones and tablets: sync to a home computer, or enable online backups (may have small cost)





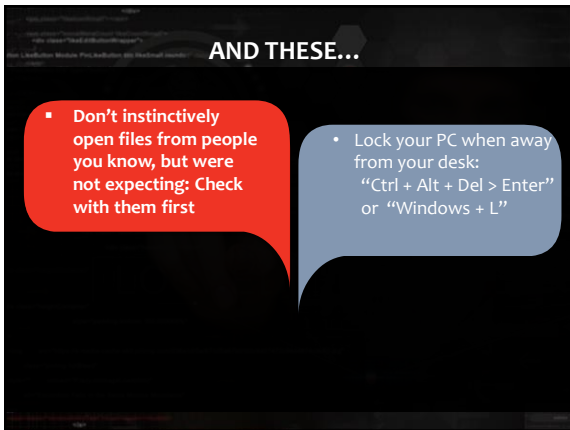


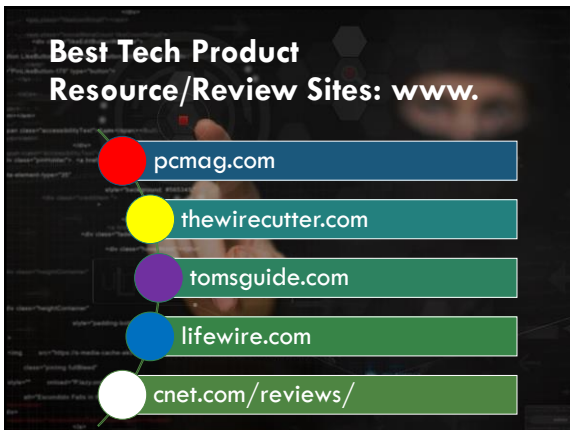












Some Personal Tech Resources

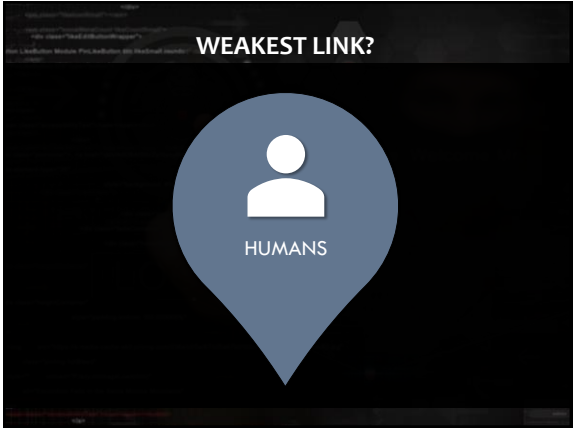
- www.Malwarebytes.com**
 - Excellent "freemium" software to keep your machine clean
- www.StopThinkConnect.org**
 - US DHS site with security resources for all ages and groups
- <http://haveibeenpwned.com>**
 - Can tell if you your email related password has been stolen

And For Your Organization...

- www.gmis.org**
 - Professional association of public sector IT managers
- www.cyber.nj.gov and MS-ISAC:
www.cisecurity.org/ms-isac/**
 - NJ Cyber Communications and Integration Cell and MS-ISAC the free federal state/local IT security support group
- SANS "OUCH" Newsletter** (search for it)
 - FREE monthly employee cybersecurity newsletter (from SANS) and "Security Awareness Tip of the Day"

**IS ANY OF THIS
100% EFFECTIVE?**











**FOR FURTHER DISCUSSION
& COMMENTS**



Marc Pfeiffer
Assistant Director
Bloustein Local Government
Research Center
Rutgers University
Marc.Pfeiffer@rutgers.edu



More Information

- Technology Risk Management Papers:
<http://blousteinlocal.rutgers.edu/managing-technology-risk/>
- Or search for "Bloustein Technology Risk"
