STAYING SAFE WITH TECHNOLOGY IN LOCAL GOVERNMENT

By: Marc Pfeiffer, Assistant Director
Bloustein Local Government Research Center
Rutgers University

Let's Talk About Technology Risk

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?"

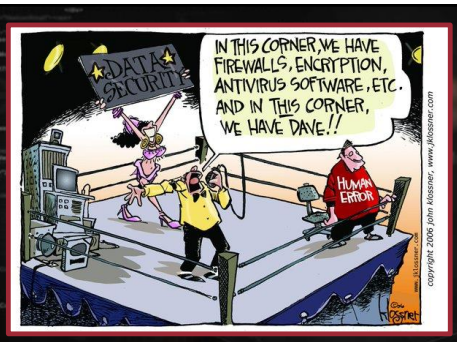
HERE'S THE CYBERSECURITY PROBLEM



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

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 Vish, 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

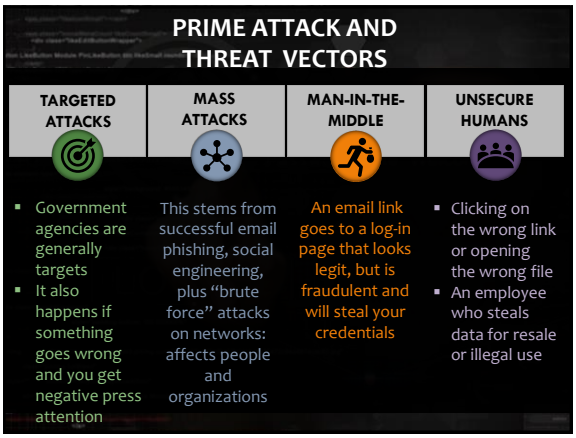
Introduce ransomware via email or network access

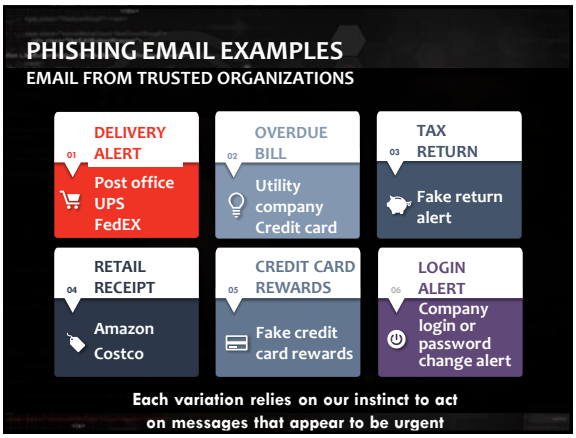
To control your system:

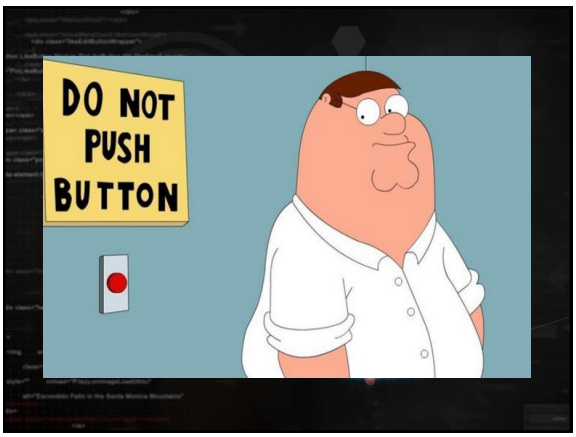
For access to data and controls

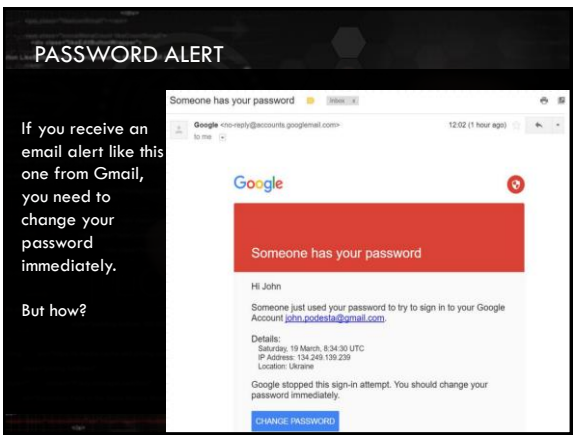
As a launching point to attack other systems;

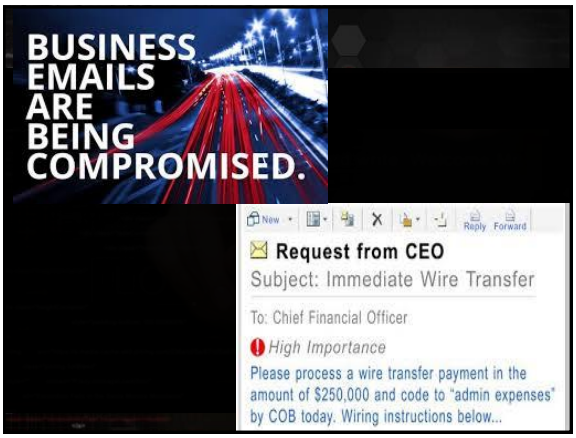
Use your processing resources for their gain

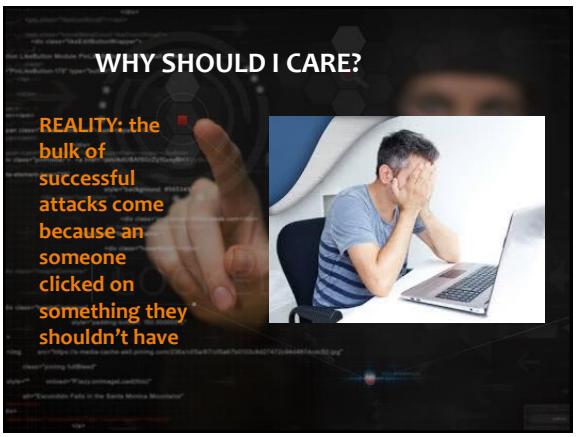


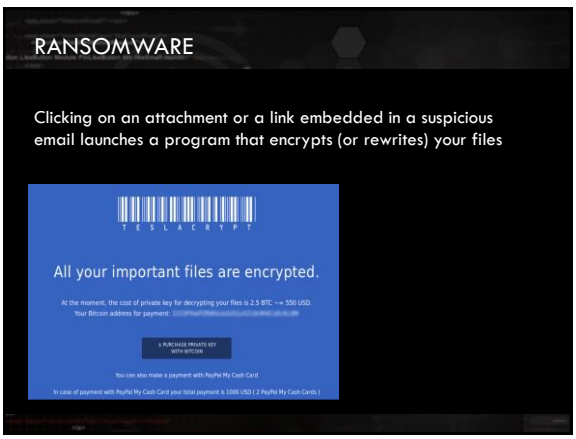


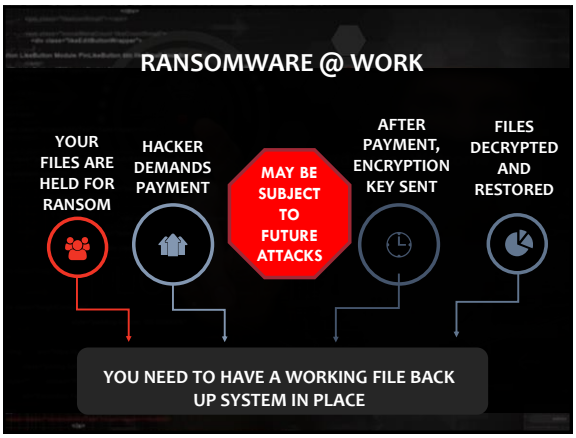


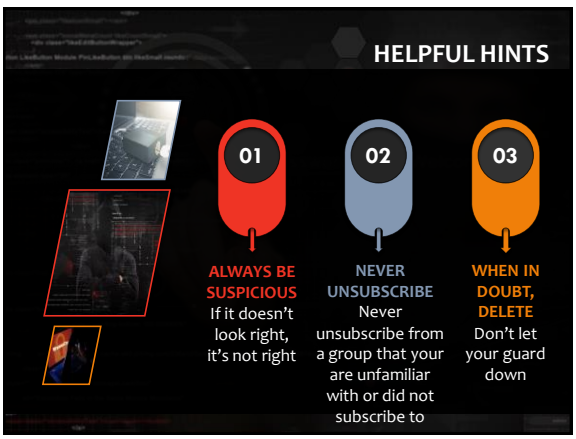


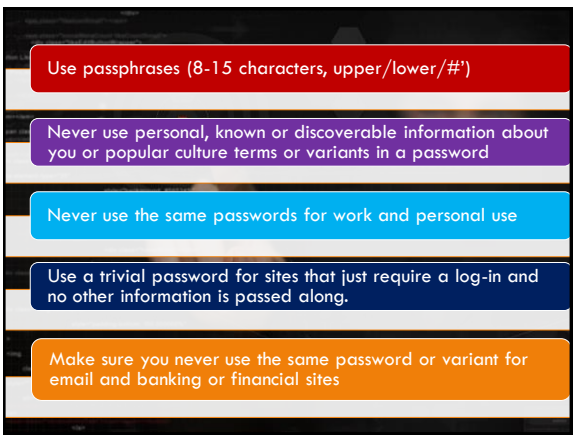








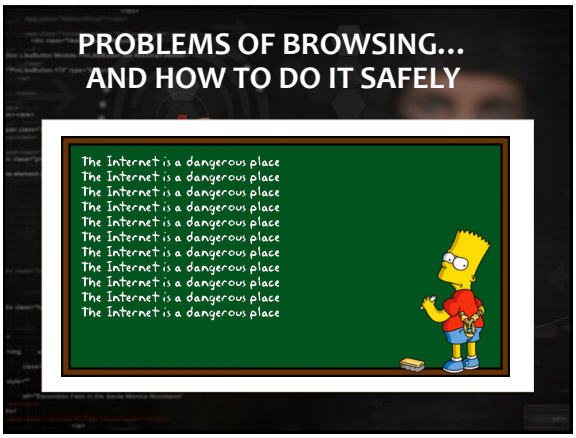


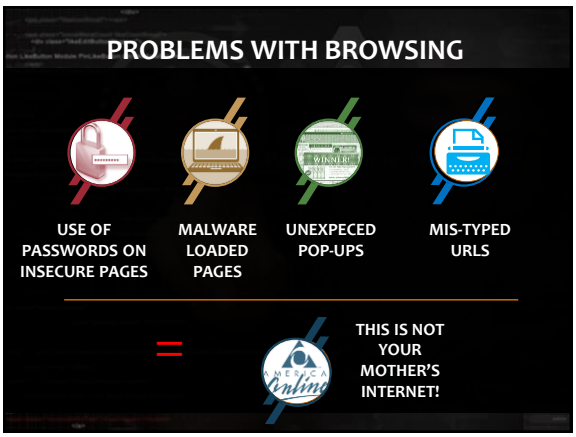


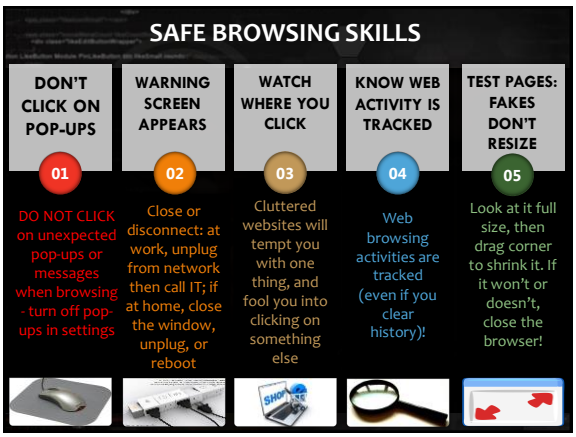
- Use two-factor authentication whenever a website offers it.
- Make sure all your devices require a password to access them
- Use the same browser and built-in password manager on devices
- Use a separate password manager program to maintain your passwords
- Only let well known websites keep your credit card information.

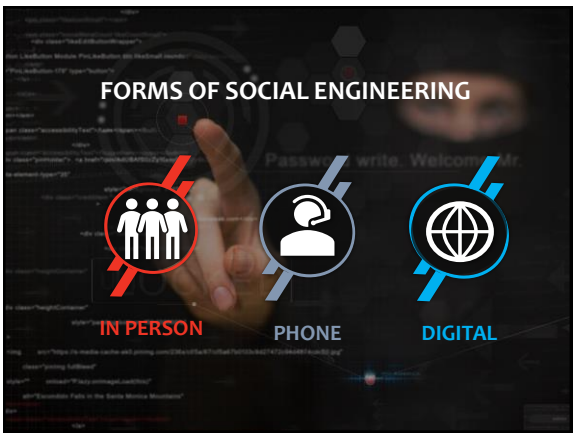
Sample Password Manager Programs

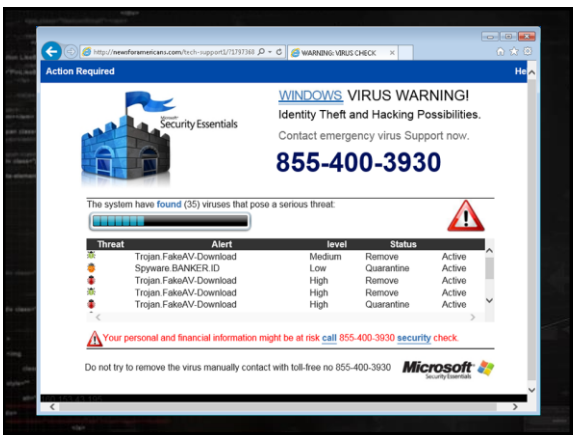
- LastPass
- Dashlane
- SplashID
- 1Passsword
- Keeper

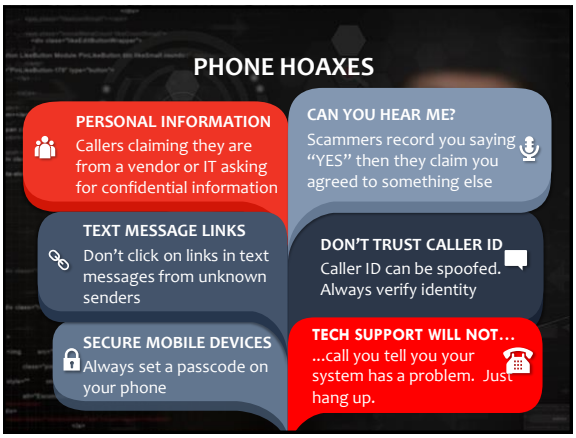


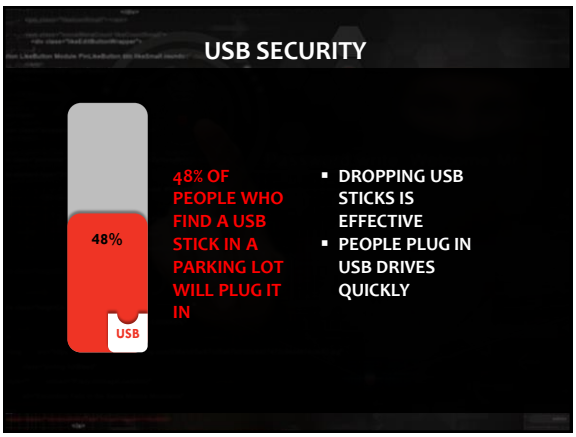


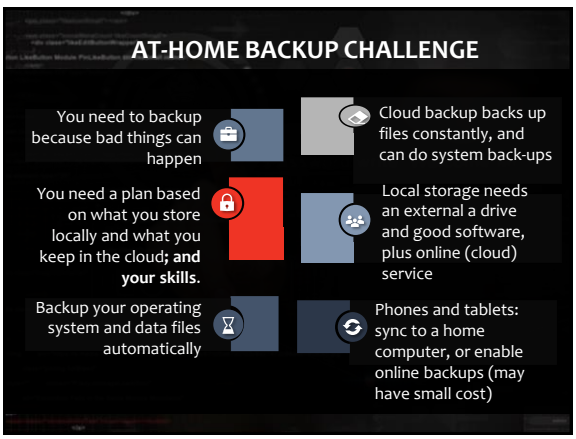






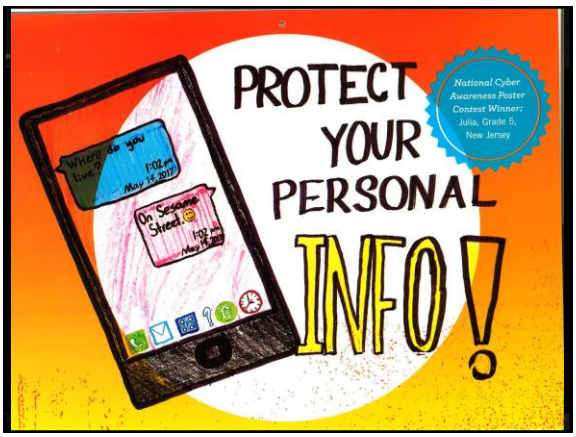






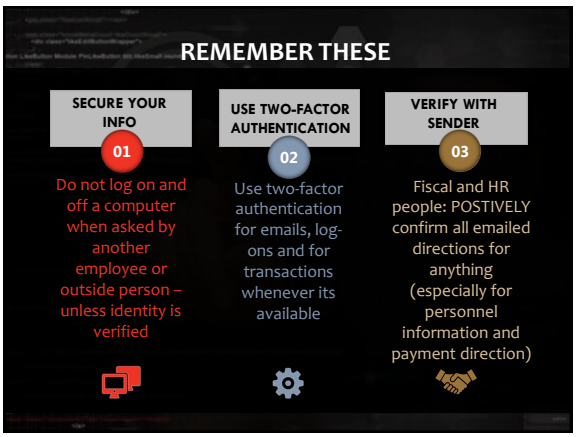
Sample Online Backup Services

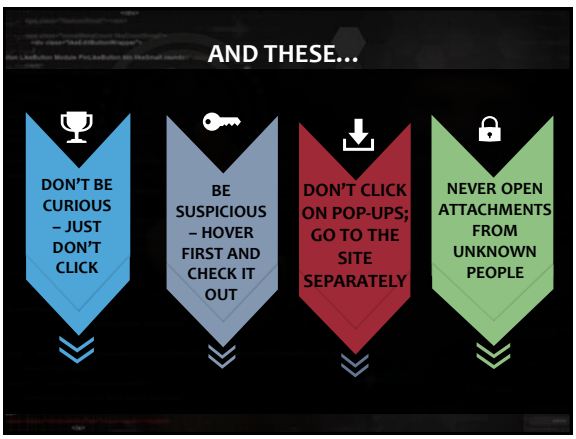
- Acronis
- Backblaze
- iDrive
- Carbonite
- Mozy
- For data files/images only: Microsoft Live and Google Drive

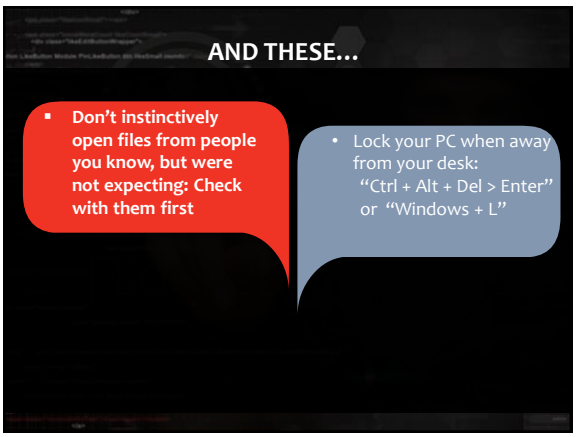


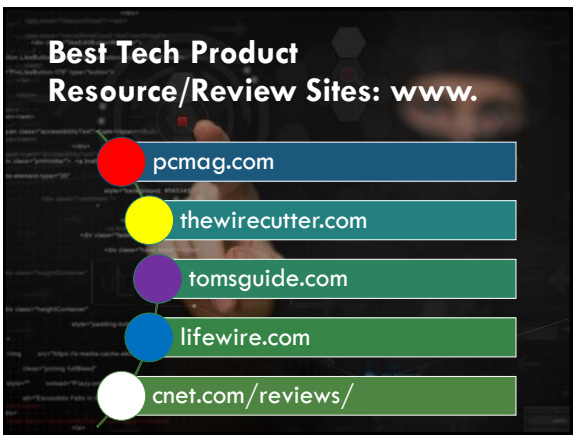
Protecting identity: you and your kids

- Don't give out SS#'s & birthdates unless essential
- Safely store documents with PII and shred the rest
- Be sure "safe" storage is really safe
- Periodically check for credit report on kids – and you
- If a child has a report – freeze it; or create one, then freeze it.









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"