# CYBER HYGIENE FOR PRETTY MUCH ANYONE WHO USES THE INTERNET

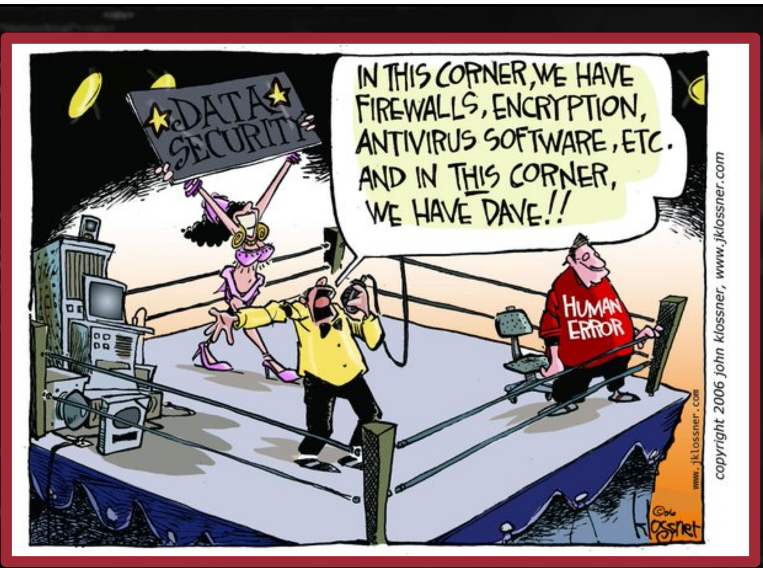
By: Marc Pfeiffer, Assistant Director
Bloustein Local Government Research Center
Rutgers University

## HERE'S THE 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


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
copyright 2006 john klossner, www.jklossner.com
www.jklossner.com
©06 Klossner

## HUMAN ERROR

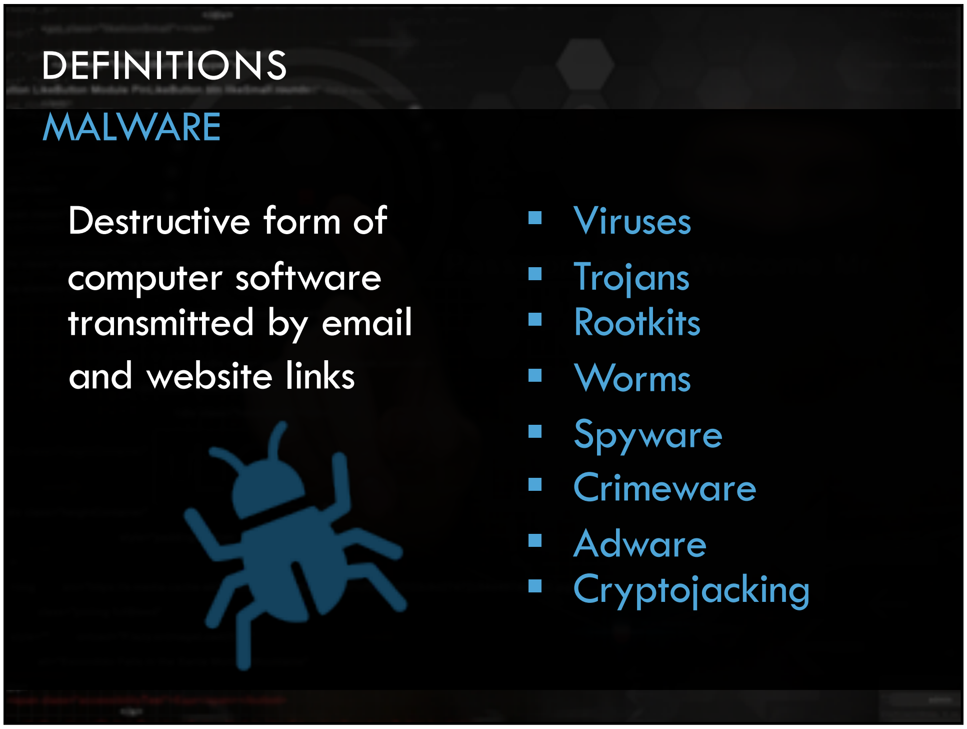
THE WEAKEST LINK

## DEFINITIONS

## SOCIAL ENGINEERING

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

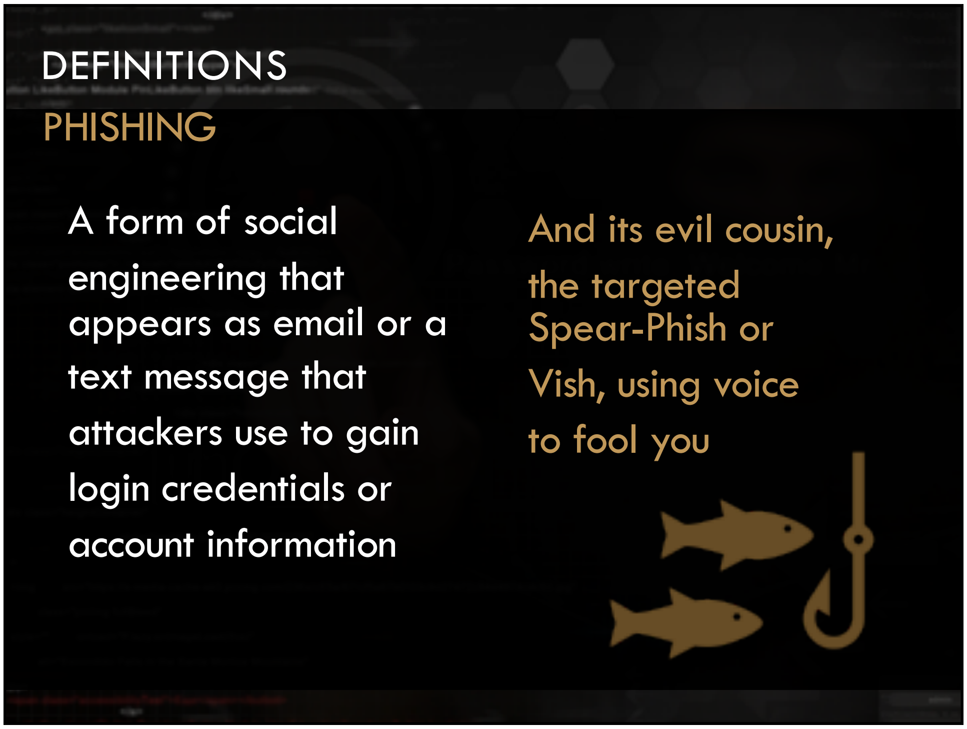
- Fraud
- Deceit
- Fear
- Greed



## DEFINITIONS
### MALWARE

Destructive form of computer software transmitted by email and website links

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

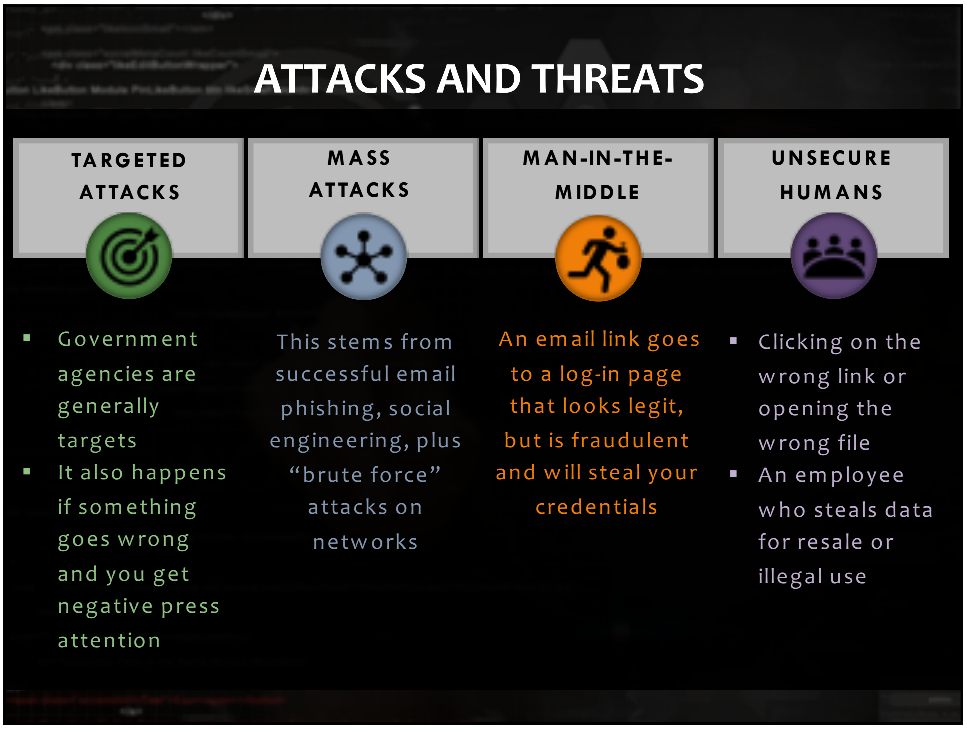


## DEFINITIONS
### PHISHING

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

# TYPES OF ATTACKS AND THREATS



# ATTACKS AND THREATS

### TARGETED ATTACKS

- Government agencies are generally targets
- It also happens if something goes wrong and you get negative press attention

### MASS ATTACKS

This stems from successful email phishing, social engineering, plus “brute force” attacks on networks

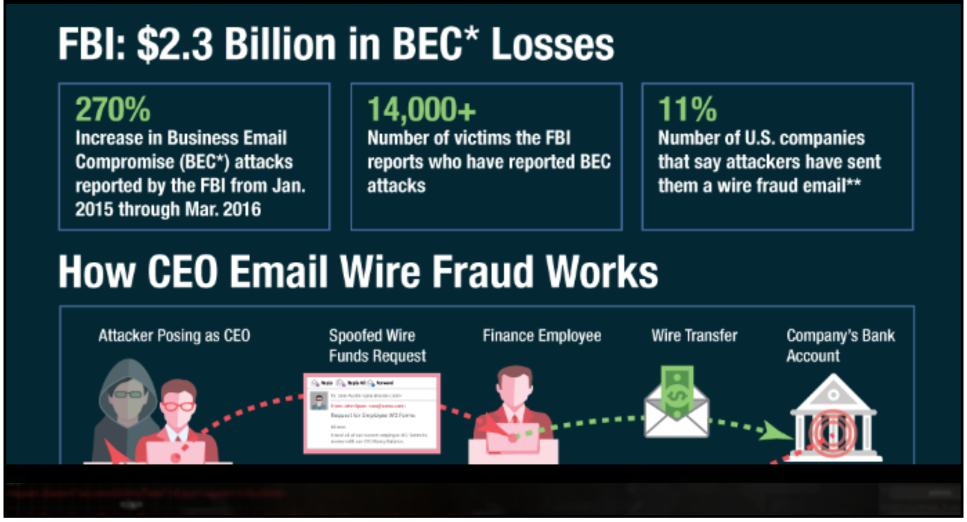
### MAN-IN-THE-MIDDLE

An email link goes to a log-in page that looks legit, but is fraudulent and will steal your credentials

### UNSECURE HUMANS

- Clicking on the wrong link or opening the wrong file
- An employee who steals data for resale or illegal use

## BUSINESS EMAIL COMPROMISE



FBI: $2.3 Billion in BEC* Losses

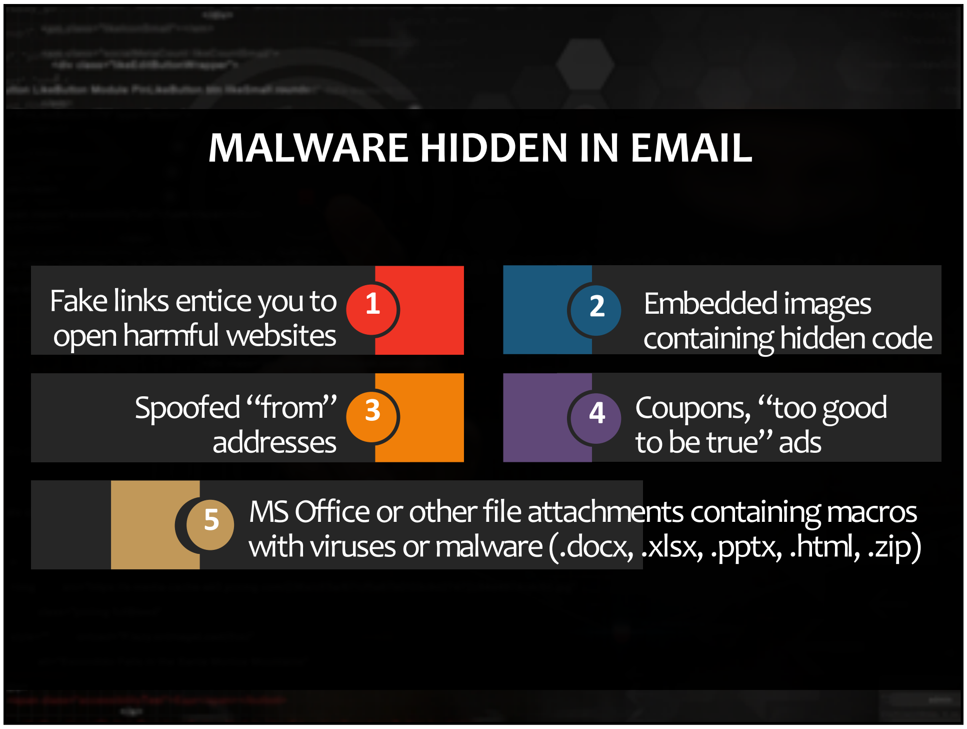
270%
Increase in Business Email Compromise (BEC*) attacks reported by the FBI from Jan. 2015 through Mar. 2016

14,000+
Number of victims the FBI reports who have reported BEC attacks

11%
Number of U.S. companies that say attackers have sent them a wire fraud email**

How CEO Email Wire Fraud Works

## WHEN EMAIL TURNS EVIL



## MALWARE HIDDEN IN EMAIL

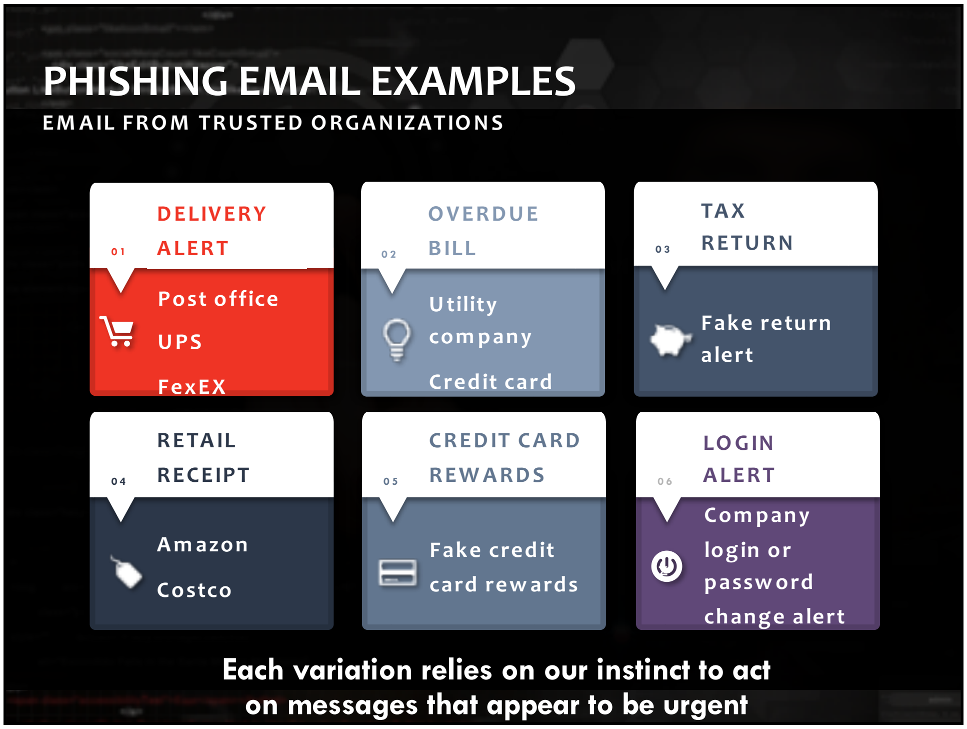
1 Fake links entice you to open harmful websites

2 Embedded images containing hidden code

3 Spoofed "from" addresses

4 Coupons, "too good to be true" ads

5 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
- FexEX

02 OVERDUE BILL
- Utility company
- Credit card

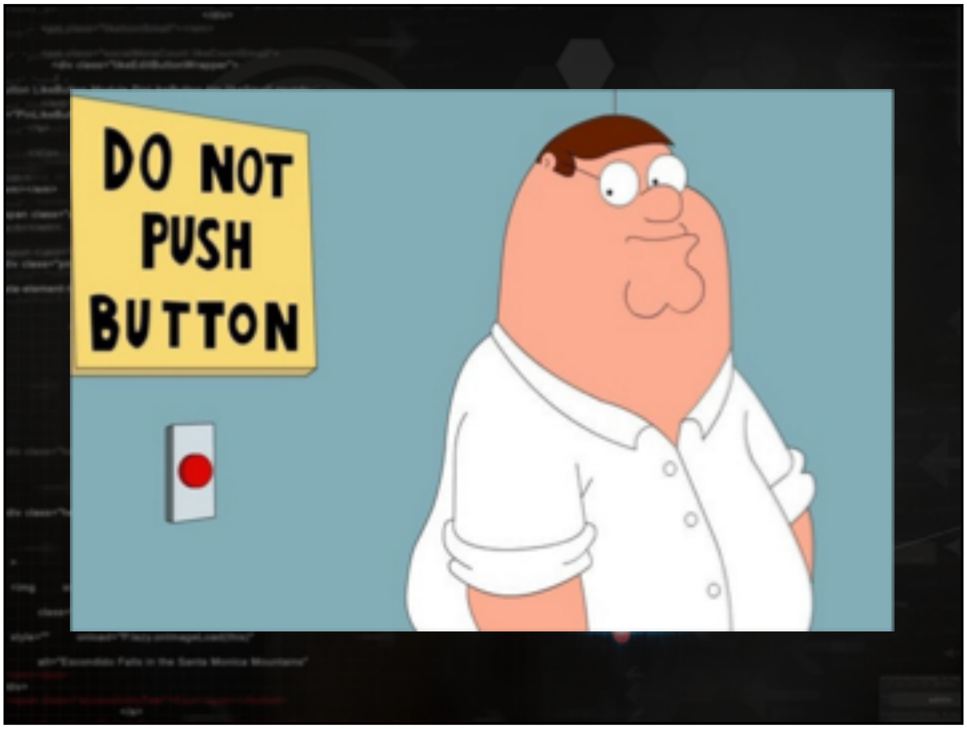
03 TAX RETURN
- Fake return alert

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**



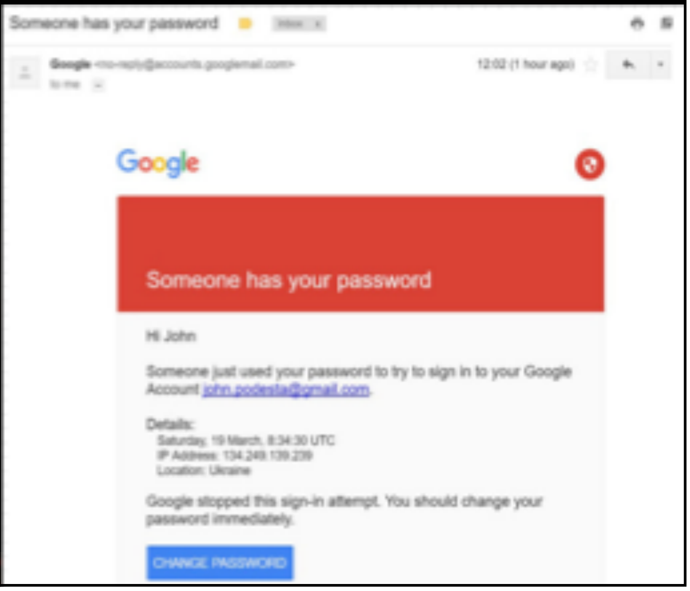
## WHY SHOULD I CARE?

REALITY: the bulk of successful attacks come because an employee clicked on something they shouldn't have

## PASSWORD ALERT

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

But how?



Someone has your password

Google <no-reply@accounts.googlemail.com>
to me

12:02 (1 hour ago)

Someone has your password

Hi John

Someone just used your password to try to sign in to your Google Account john.podesta@gmail.com.

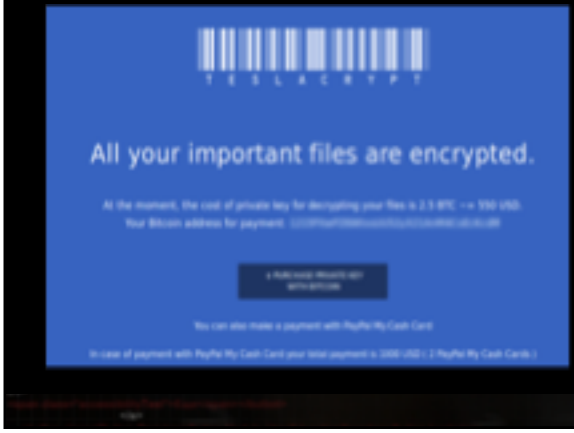
Details:
Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

CHANGE PASSWORD

## RANSOMWARE

Clicking on an attachment or a link embedded in a suspicious email launches a program that encrypts (or rewrites) your files



TESLACRYPT

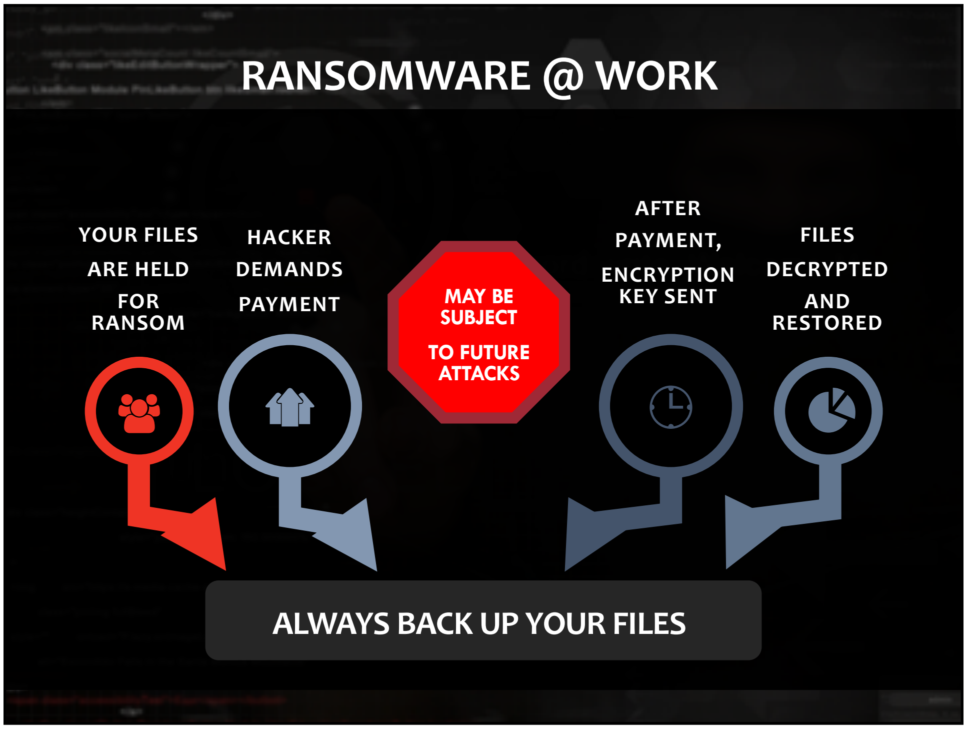
All your important files are encrypted.

At the moment, the cost of private key for decrypting your files is 2.5 BTC ~= 550 USD.
Your Bitcoin address for payment: [illegible]

Purchase private key with Bitcoin

You can also make a payment with PayPal My Cash Card

In case of payment with PayPal My Cash Card your total payment is 1000 USD (2 PayPal My Cash Cards.)



## RANSOMWARE @ WORK

YOUR FILES ARE HELD FOR RANSOM

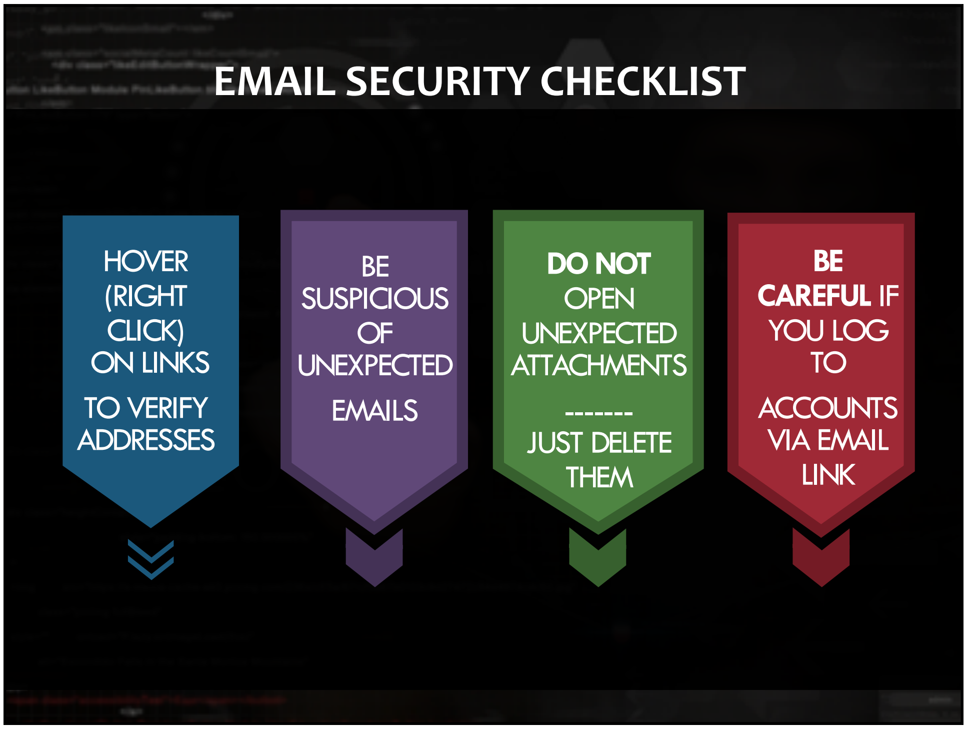
HACKER DEMANDS PAYMENT

MAY BE SUBJECT TO FUTURE ATTACKS

AFTER PAYMENT, ENCRYPTION KEY SENT

FILES DECRYPTED AND RESTORED

ALWAYS BACK UP YOUR FILES



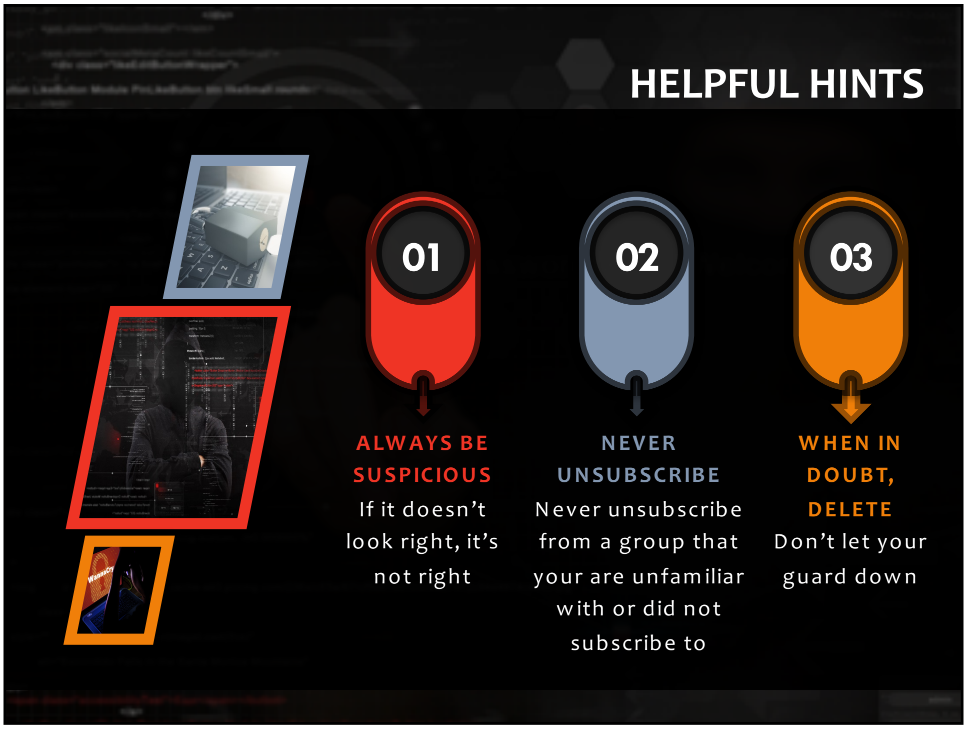
## EMAIL SECURITY CHECKLIST

HOVER (RIGHT CLICK) ON LINKS TO VERIFY ADDRESSES

BE SUSPICIOUS OF UNEXPECTED EMAILS

**DO NOT** OPEN UNEXPECTED ATTACHMENTS
-------
JUST DELETE THEM

**BE CAREFUL** IF YOU LOG TO ACCOUNTS VIA EMAIL LINK



## HELPFUL HINTS

01

**ALWAYS BE SUSPICIOUS**

If it doesn’t look right, it’s not right

02

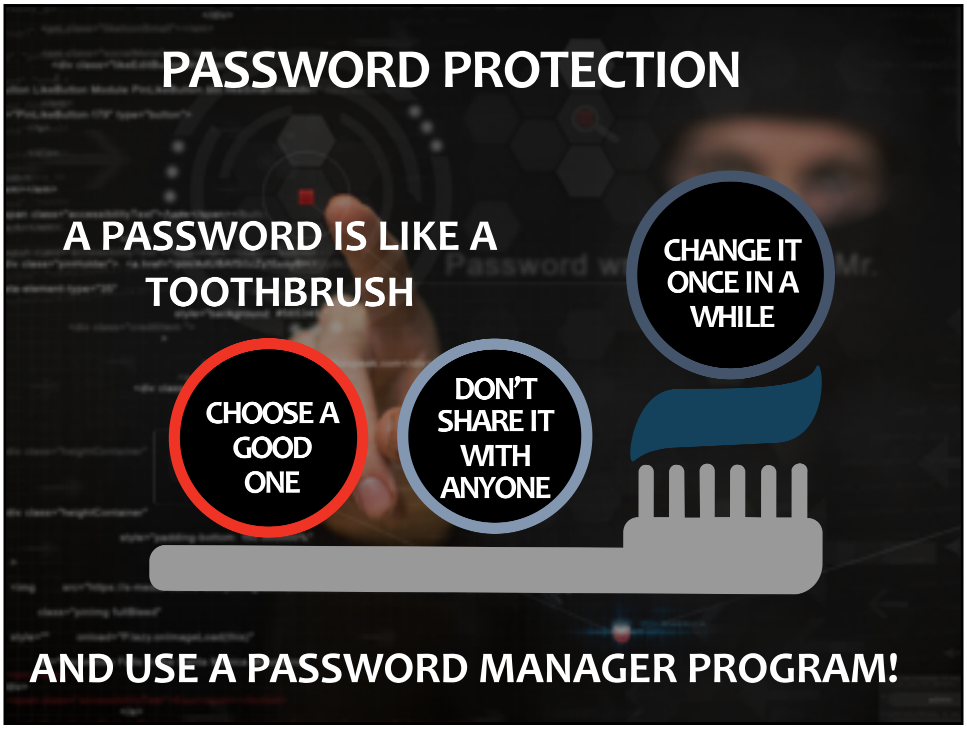
**NEVER UNSUBSCRIBE**

Never unsubscribe from a group that your are unfamiliar with or did not subscribe to

03

**WHEN IN DOUBT, DELETE**

Don’t let your guard down



## PASSWORD PROTECTION

A PASSWORD IS LIKE A TOOTHBRUSH

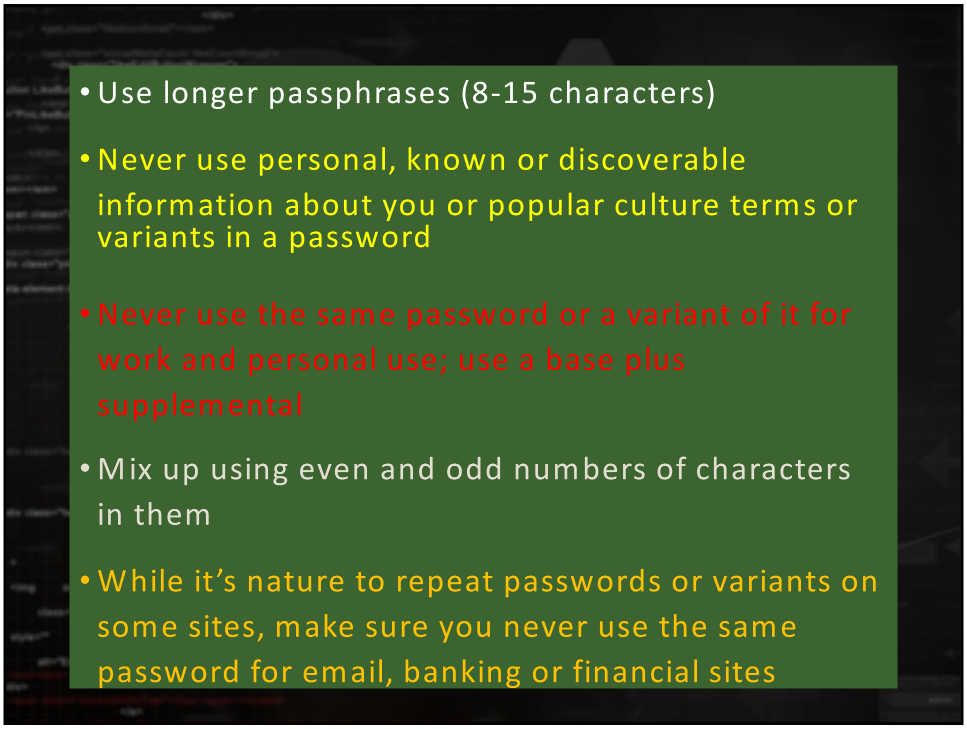
CHOOSE A GOOD ONE

DON’T SHARE IT WITH ANYONE

CHANGE IT ONCE IN A WHILE

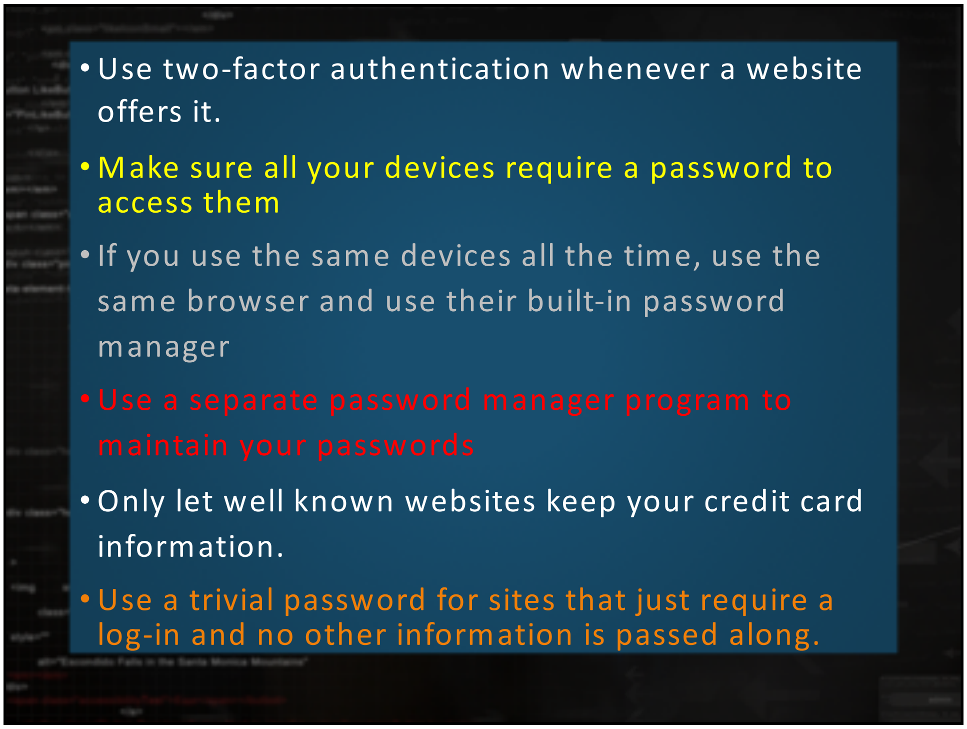
AND USE A PASSWORD MANAGER PROGRAM!

# SMART PASSWORD CONSTRUCTION



- Use longer passphrases (8-15 characters)
- Never use personal, known or discoverable information about you or popular culture terms or variants in a password
- Never use the same password or a variant of it for work and personal use; use a base plus supplemental
- Mix up using even and odd numbers of characters in them
- While it’s nature to repeat passwords or variants on some sites, make sure you never use the same password for email, banking or financial sites

# MANAGE YOUR PASSWORD ONLINE



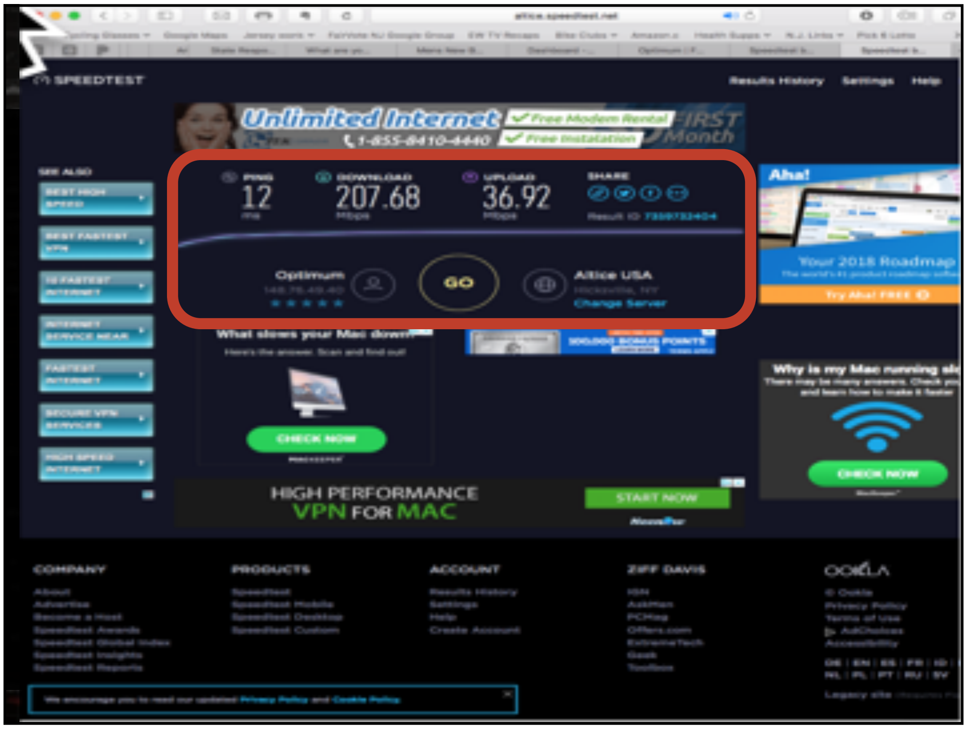
- Use two-factor authentication whenever a website offers it.
- Make sure all your devices require a password to access them
- If you use the same devices all the time, use the same browser and use their built-in password manager
- Use a separate password manager program to maintain your passwords
- Only let well known websites keep your credit card information.
- Use a trivial password for sites that just require a log-in and no other information is passed along.

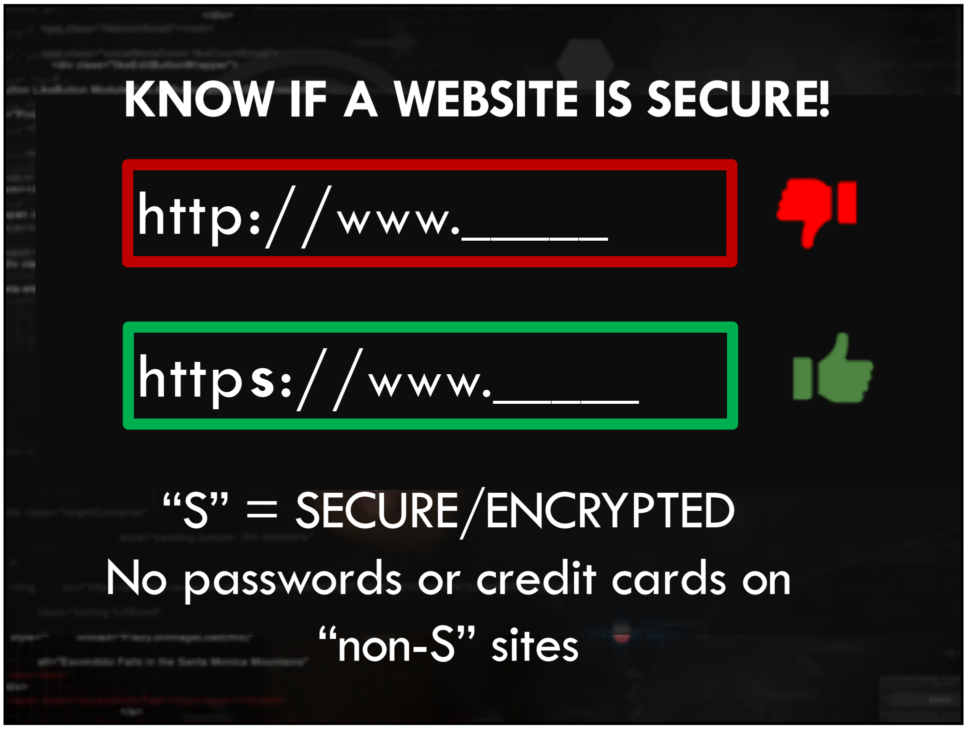
## PROBLEMS OF BROWSING… AND HOW TO DO IT SAFELY

The Internet is a dangerous place
The Internet is a dangerous place
The Internet is a dangerous place
The Internet is a dangerous place
The Internet is a dangerous place
The Internet is a dangerous place
The Internet is a dangerous place
The Internet is a dangerous place
The Internet is a dangerous place
The Internet is a dangerous place
The Internet is a dangerous place

## PROBLEMS WITH BROWSING

- USE OF PASSWORDS ON INSECURE PAGES
- MALWARE LOADED PAGES
- UNEXPECED POP-UPS
- THIS IS NOT YOUR MOTHER'S INTERNET!





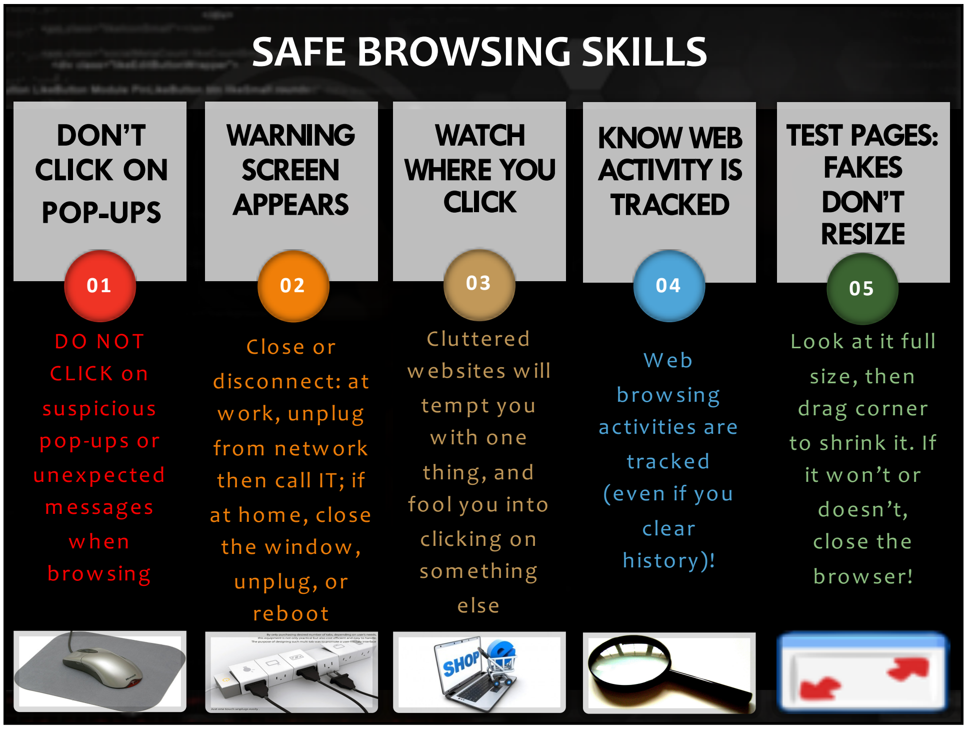
## KNOW IF A WEBSITE IS SECURE!

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**

01

DO NOT CLICK on suspicious pop-ups or unexpected messages when browsing

**WARNING SCREEN APPEARS**

02

Close or disconnect: at work, unplug from network then call IT; if at home, close the window, unplug, or reboot

**WATCH WHERE YOU CLICK**

03

Cluttered websites will tempt you with one thing, and fool you into clicking on something else

**KNOW WEB ACTIVITY IS TRACKED**

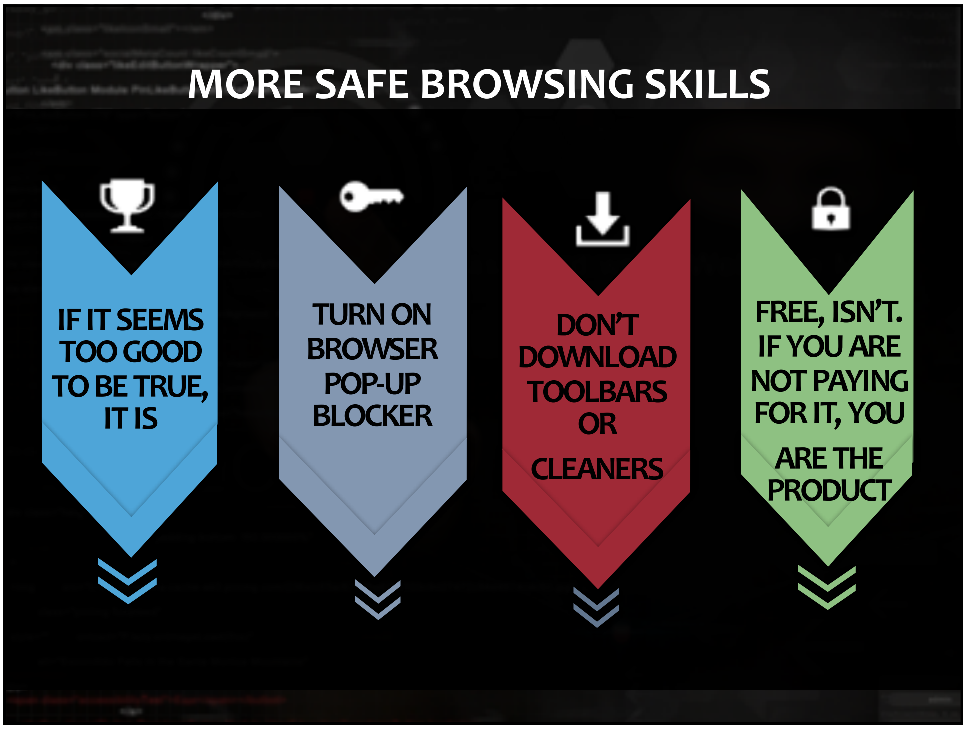
04

Web browsing activities are tracked (even if you clear history)!

**TEST PAGES: FAKES DON'T RESIZE**

05

Look at it full size, then drag corner to shrink it. If it won't or doesn't, close the browser!



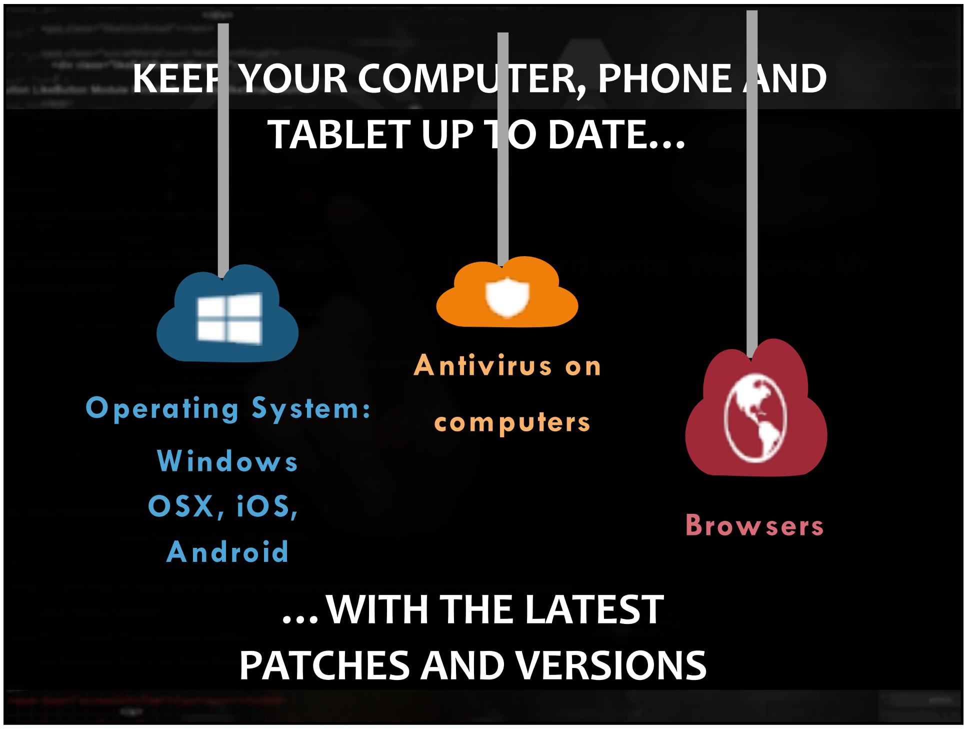
## MORE SAFE BROWSING SKILLS

**IF IT SEEMS TOO GOOD TO BE TRUE, IT IS**

**TURN ON BROWSER POP-UP BLOCKER**

**DON'T DOWNLOAD TOOLBARS OR CLEANERS**

**FREE, ISN'T. IF YOU ARE NOT PAYING FOR IT, YOU ARE THE PRODUCT**



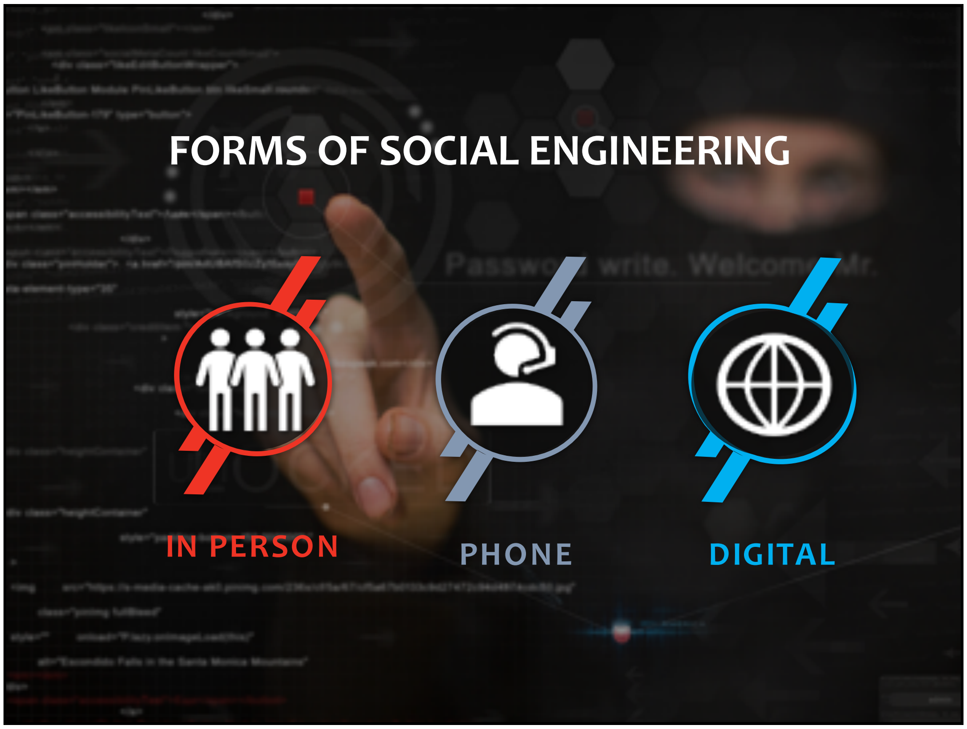
## KEEP YOUR COMPUTER, PHONE AND TABLET UP TO DATE…

Operating System:
Windows
OSX, iOS,
Android

Antivirus on computers

Browsers

…WITH THE LATEST PATCHES AND VERSIONS

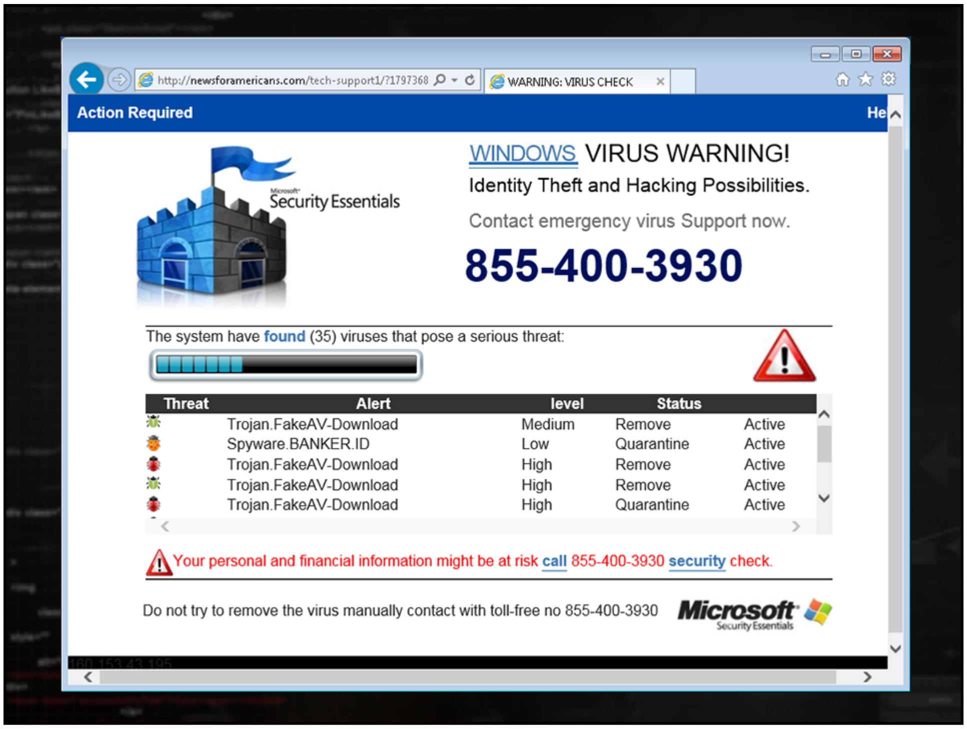


## FORMS OF SOCIAL ENGINEERING

IN PERSON

PHONE

DIGITAL


http://newsforamericans.com/tech-support1/?1797368
WARNING: VIRUS CHECK
Action Required
He
Microsoft Security Essentials
Microsoft Security Essentials

WINDOWS VIRUS WARNING!

Identity Theft and Hacking Possibilities.

Contact emergency virus Support now.

855-400-3930

The system have found (35) viruses that pose a serious threat:

| Threat | Alert | level | Status | |
|---|---|---|---|---|
| | Trojan.FakeAV-Download | Medium | Remove | Active |
| | Spyware.BANKER.ID | Low | Quarantine | Active |
| | Trojan.FakeAV-Download | High | Remove | Active |
| | Trojan.FakeAV-Download | High | Remove | Active |
| | Trojan.FakeAV-Download | High | Quarantine | Active |

Your personal and financial information might be at risk call 855-400-3930 security check.

Do not try to remove the virus manually contact with toll-free no 855-400-3930

## PHONE HOAXES

**PERSONAL INFORMATION**

Callers claiming they are from a vendor or IT asking for confidential information

**CAN YOU HEAR ME?**

Scammers record you saying "YES" then they claim you agreed to something else

**TEXT MESSAGE LINKS**

Don't click on links in text messages from unknown senders

**DON'T TRUST CALLER ID**

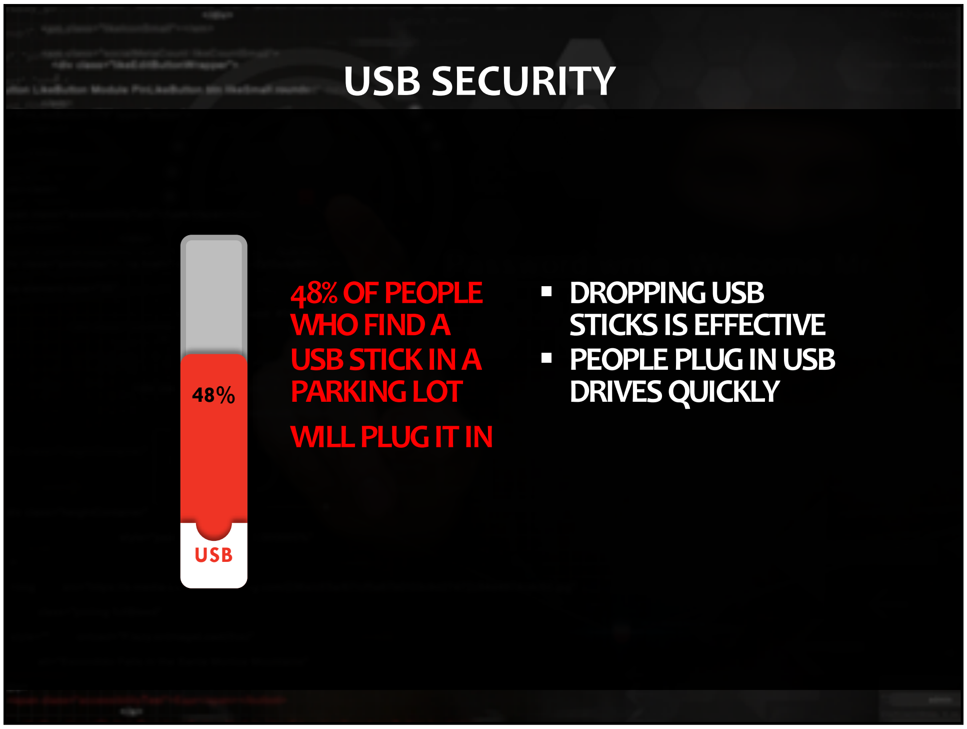
Caller ID can be spoofed. Always verify identity

**SECURE MOBILE DEVICES**

Always set a passcode on your phone

**TECH SUPPORT WILL NOT…**

…call you tell you your system has a problem. Just hang up.

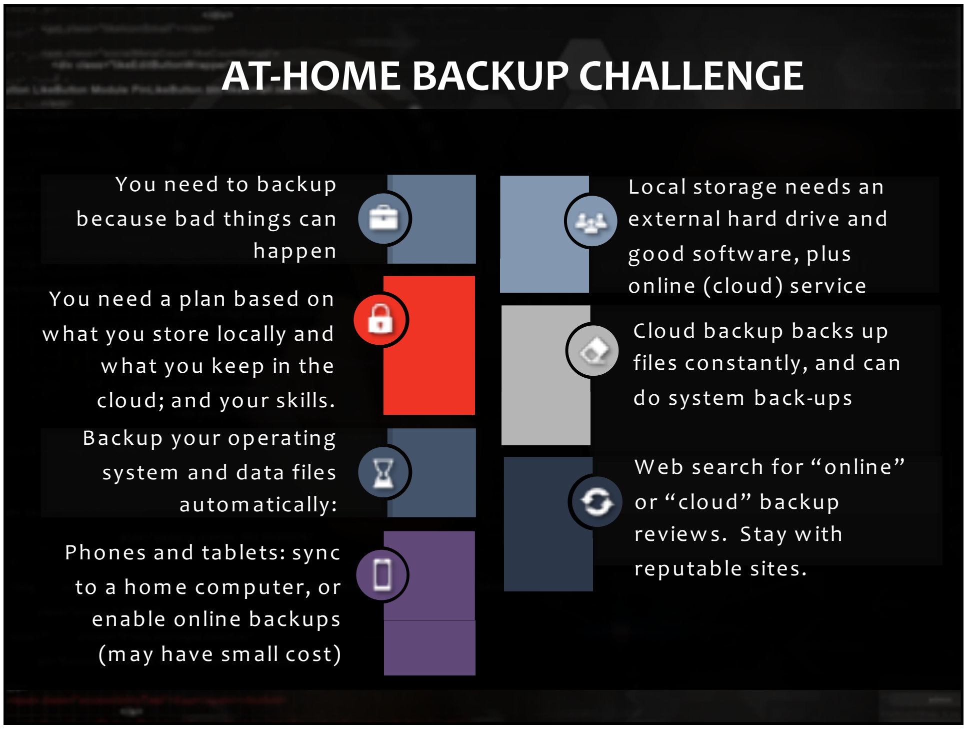


## USB SECURITY

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.

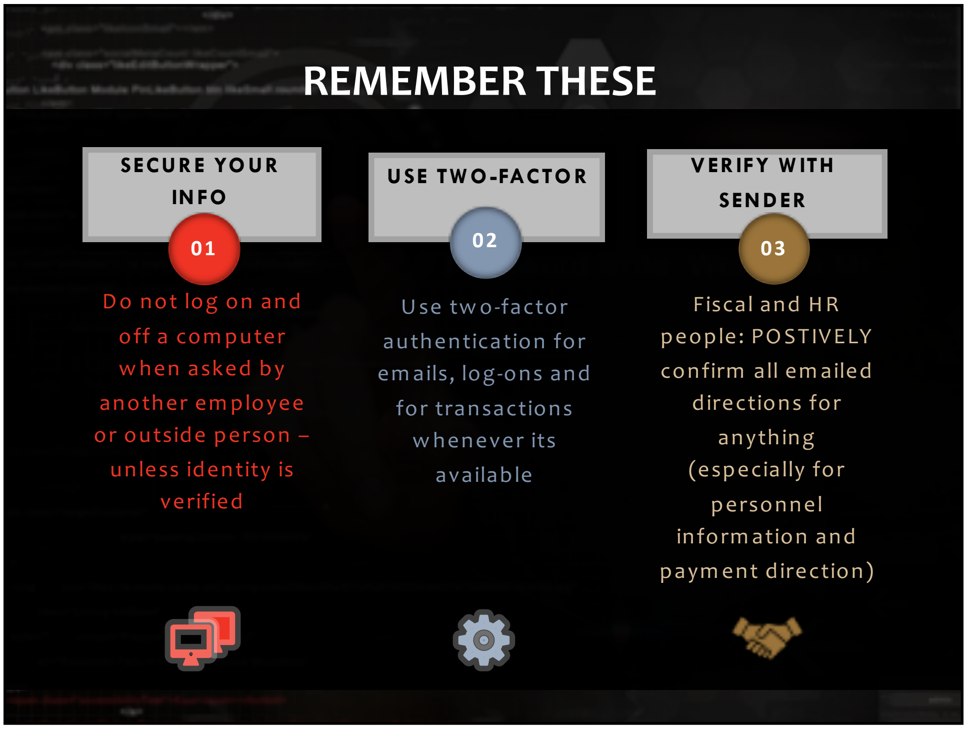
Backup your operating system and data files automatically:

Phones and tablets: sync to a home computer, or enable online backups (may have small cost)

Local storage needs an external hard drive and good software, plus online (cloud) service

Cloud backup backs up files constantly, and can do system back-ups

Web search for “online” or “cloud” backup reviews. Stay with reputable sites.



## REMEMBER THESE

SECURE YOUR INFO

01

Do not log on and off a computer when asked by another employee or outside person – unless identity is verified

USE TWO-FACTOR

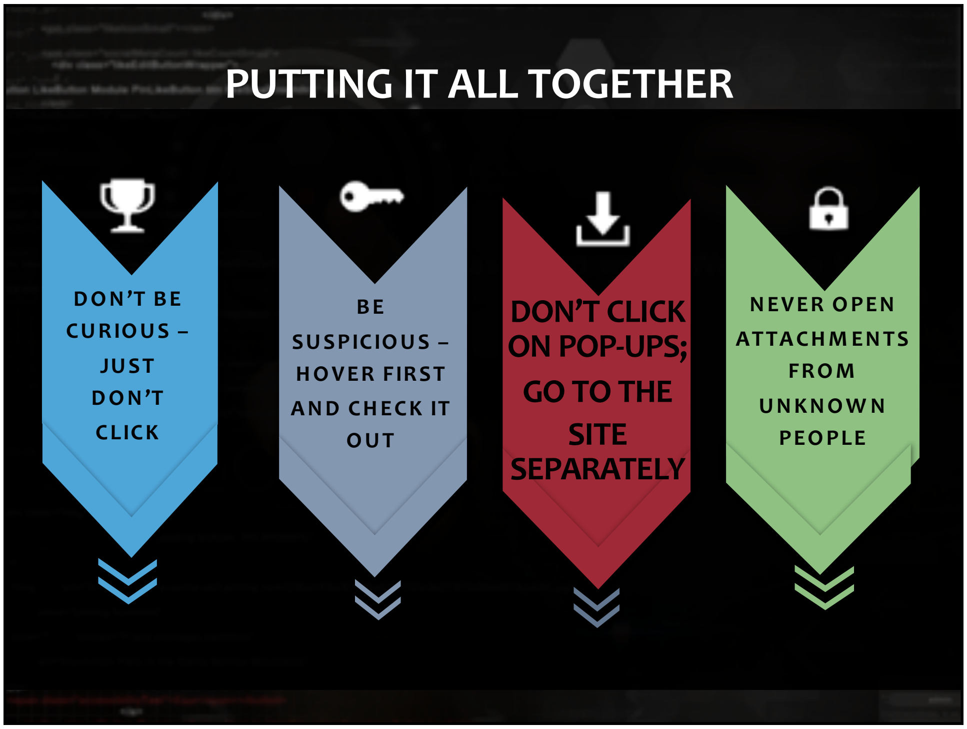
02

Use two-factor authentication for emails, log-ons and for transactions whenever its available

VERIFY WITH SENDER

03

Fiscal and HR people: POSTIVELY confirm all emailed directions for anything (especially for personnel information and payment direction)



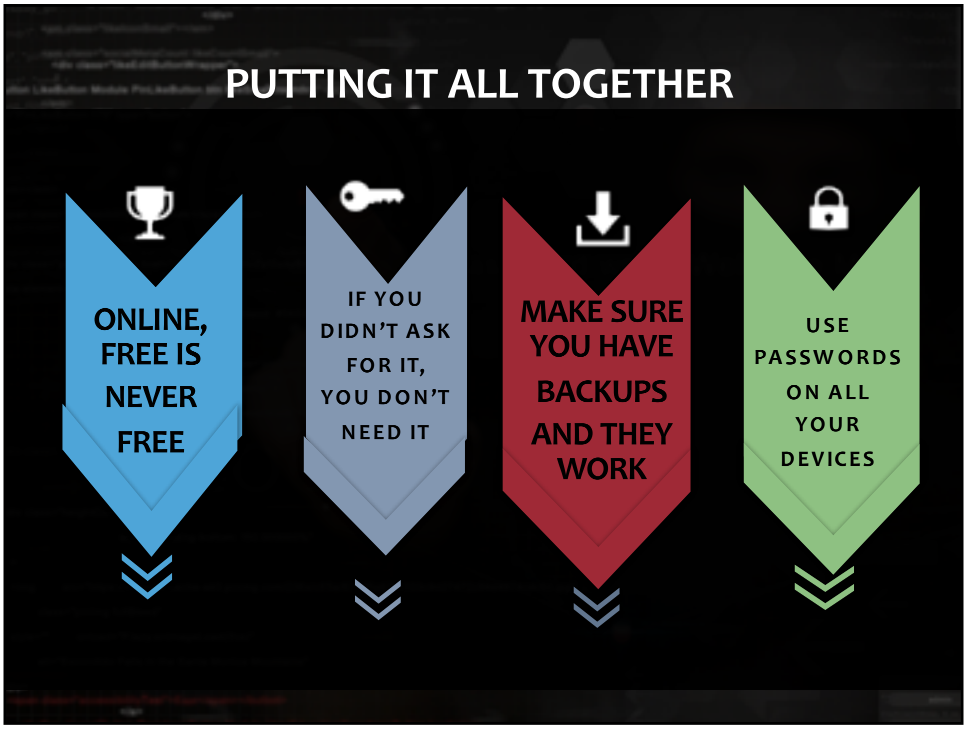
## PUTTING IT ALL TOGETHER

DON'T BE CURIOUS – JUST DON'T CLICK

BE SUSPICIOUS – HOVER FIRST AND CHECK IT OUT

DON'T CLICK ON POP-UPS; GO TO THE SITE SEPARATELY

NEVER OPEN ATTACHMENTS FROM UNKNOWN PEOPLE



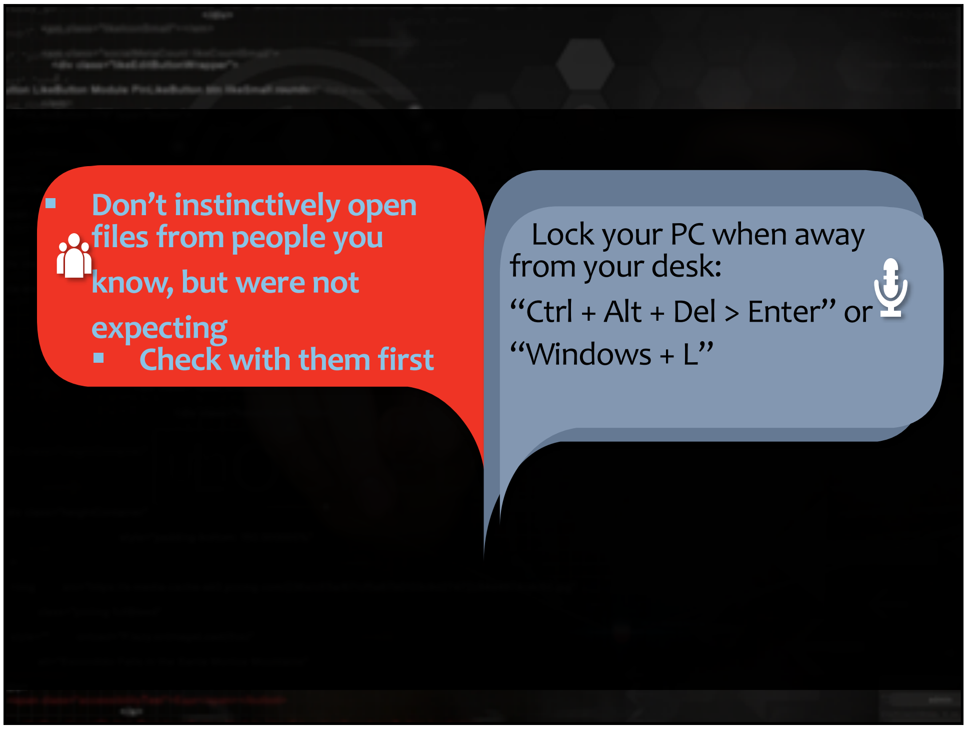
## PUTTING IT ALL TOGETHER

ONLINE, FREE IS NEVER FREE

IF YOU DIDN'T ASK FOR IT, YOU DON'T NEED IT

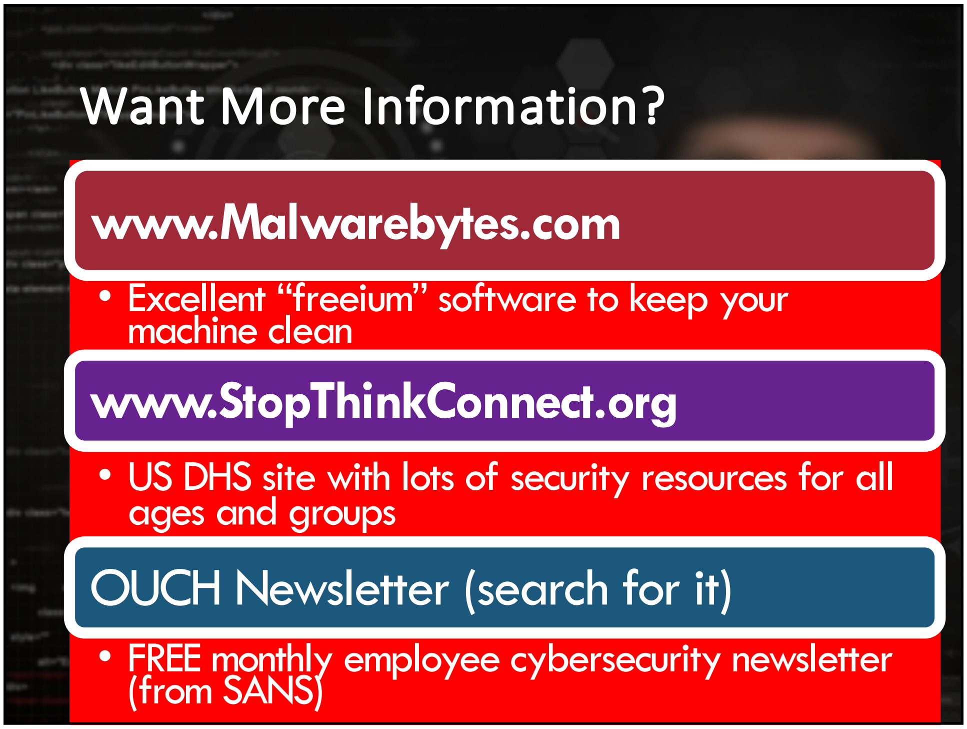
MAKE SURE YOU HAVE BACKUPS AND THEY WORK

USE PASSWORDS ON ALL YOUR DEVICES



- Don't instinctively open files from people you know, but were not expecting
  - Check with them first

Lock your PC when away from your desk:
"Ctrl + Alt + Del > Enter" or "Windows + L"



## Want More Information?

**www.Malwarebytes.com**

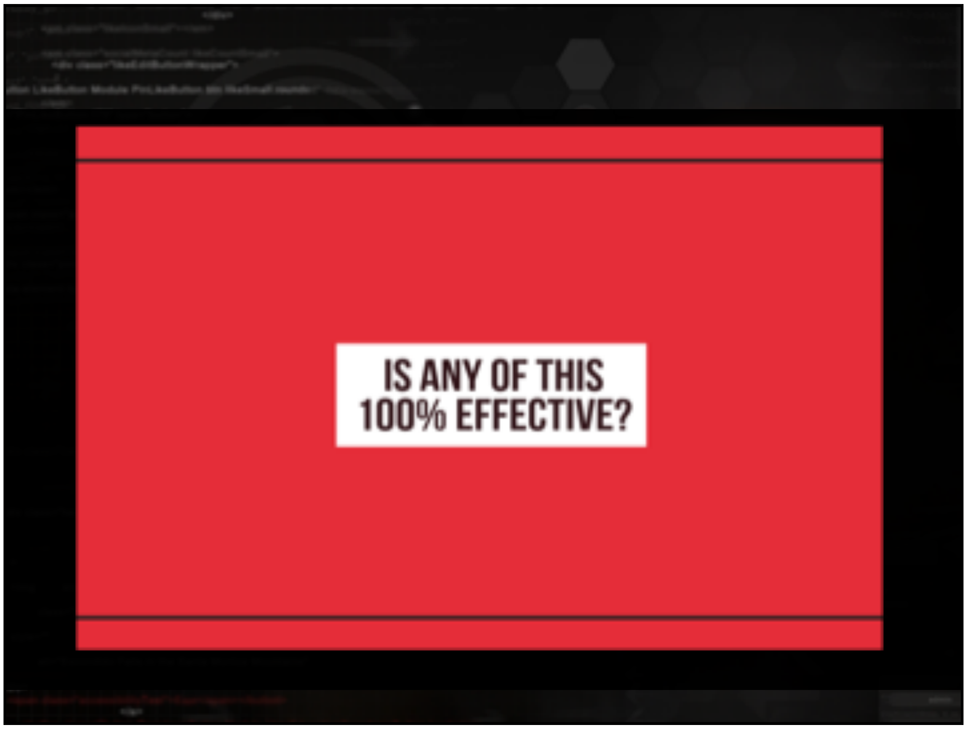
- Excellent "freeium" software to keep your machine clean

**www.StopThinkConnect.org**

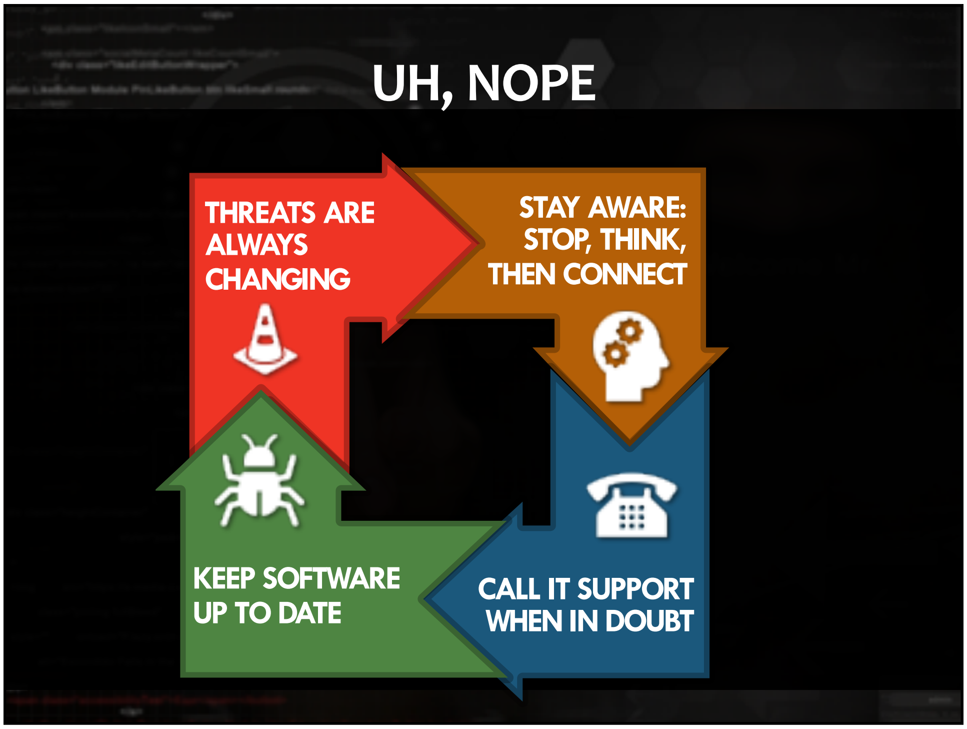
- US DHS site with lots of security resources for all ages and groups

OUCH Newsletter (search for it)

- FREE monthly employee cybersecurity newsletter (from SANS)



IS ANY OF THIS
100% EFFECTIVE?



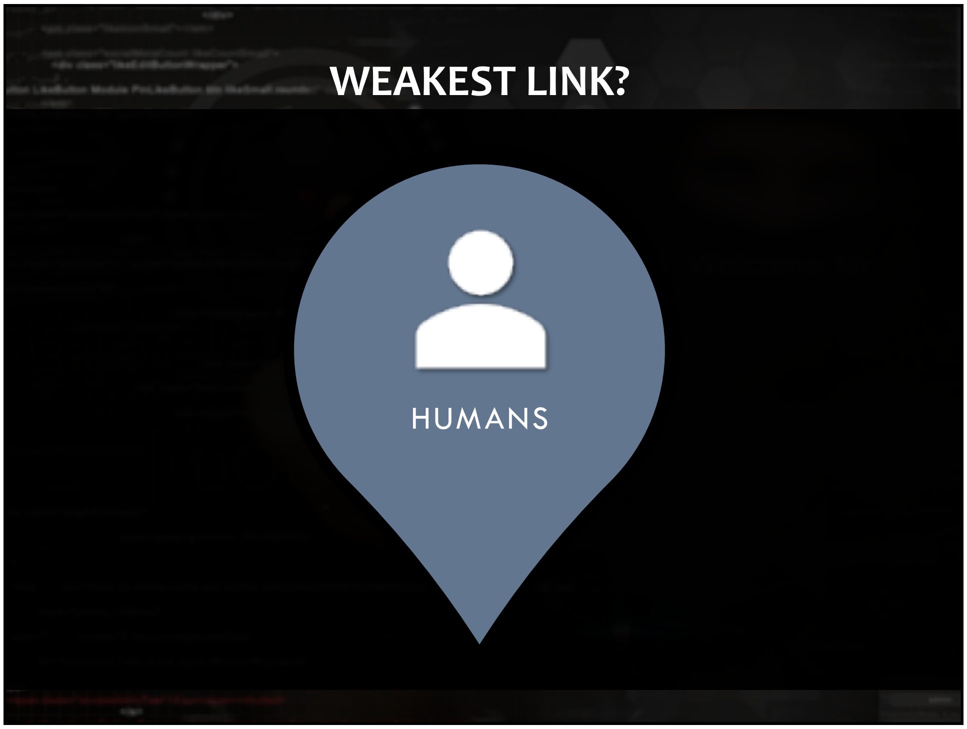
## UH, NOPE

THREATS ARE ALWAYS CHANGING

STAY AWARE: STOP, THINK, THEN CONNECT

CALL IT SUPPORT WHEN IN DOUBT

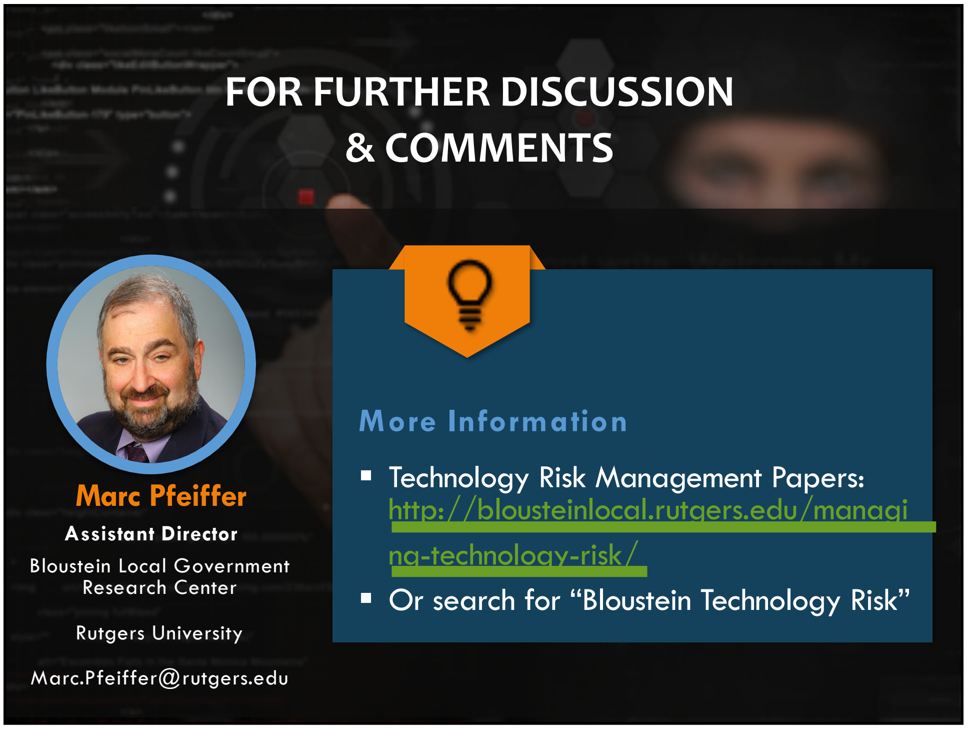
KEEP SOFTWARE UP TO DATE



## WEAKEST LINK?

HUMANS

YOU KNOW WHAT THEY SAY…



## 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"