fissea
Federal Information Systems Security Educators' Association
AWARENESS • TRAINING • EDUCATION

24th Annual Conference
Bridging to the Future –
Emerging Trends in Cybersecurity

Information System Technology When and How To Address Security Implications of New Technologies

Dr. Paul Krasley, CPLP
Defense Intelligence Agency

John Ippolito, CISSP, PMP
Allied Technology Group, Inc.

How soon should we add new technologies or new uses of technology to our awareness and training programs?

Mobile computing

Smart phones

Flash Drives

Social Networking

Blogs

Twitter

Online acquisitions

E-hiring/Electronic resumes

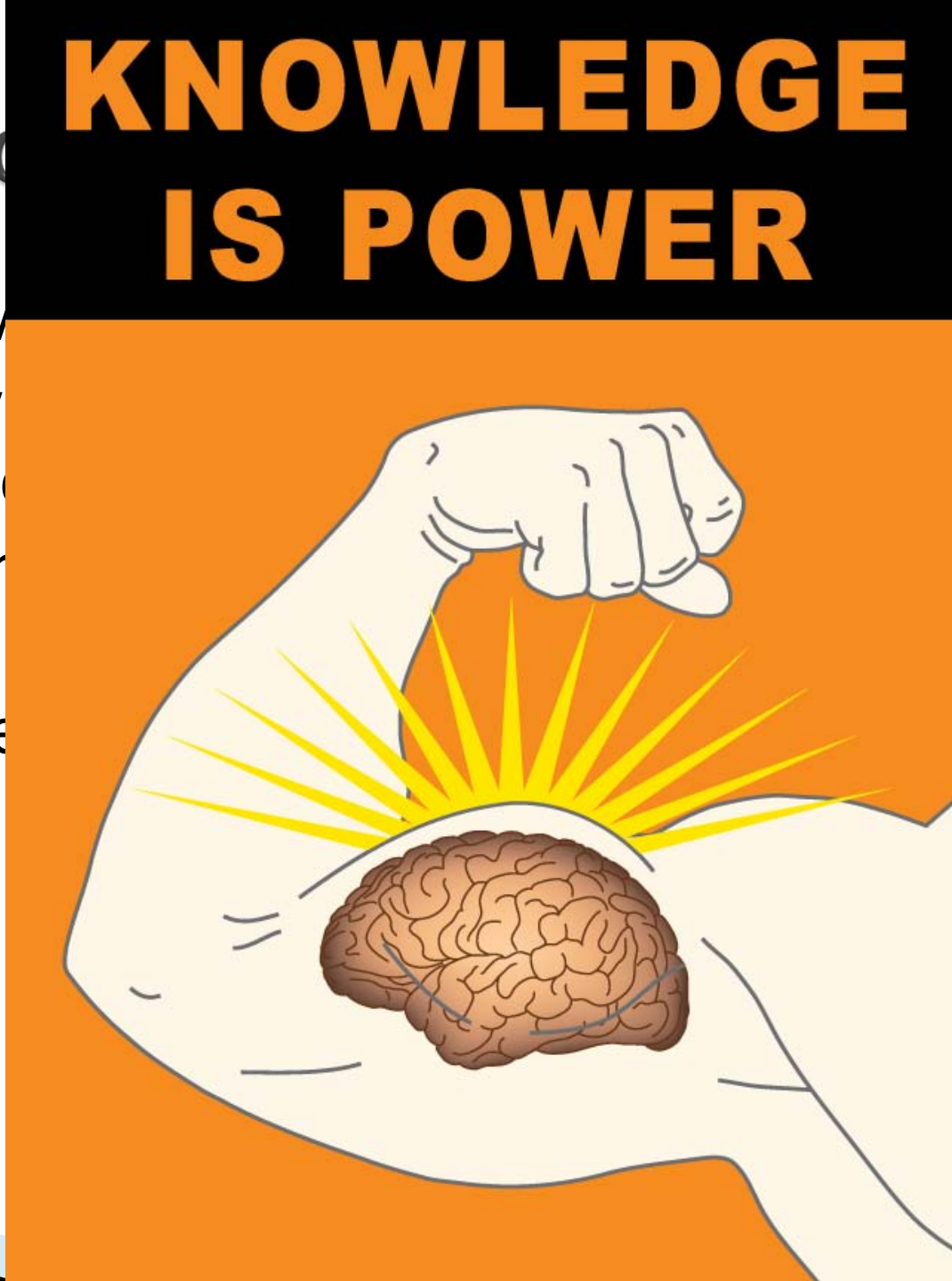
Cookies

iPads and tablets

Encryption

What do we d

- Prohibit use of new
- Train for the last w
  how to secure last
- “One size fits all” tr
  cost low. Doesn’t
- Add to training afte



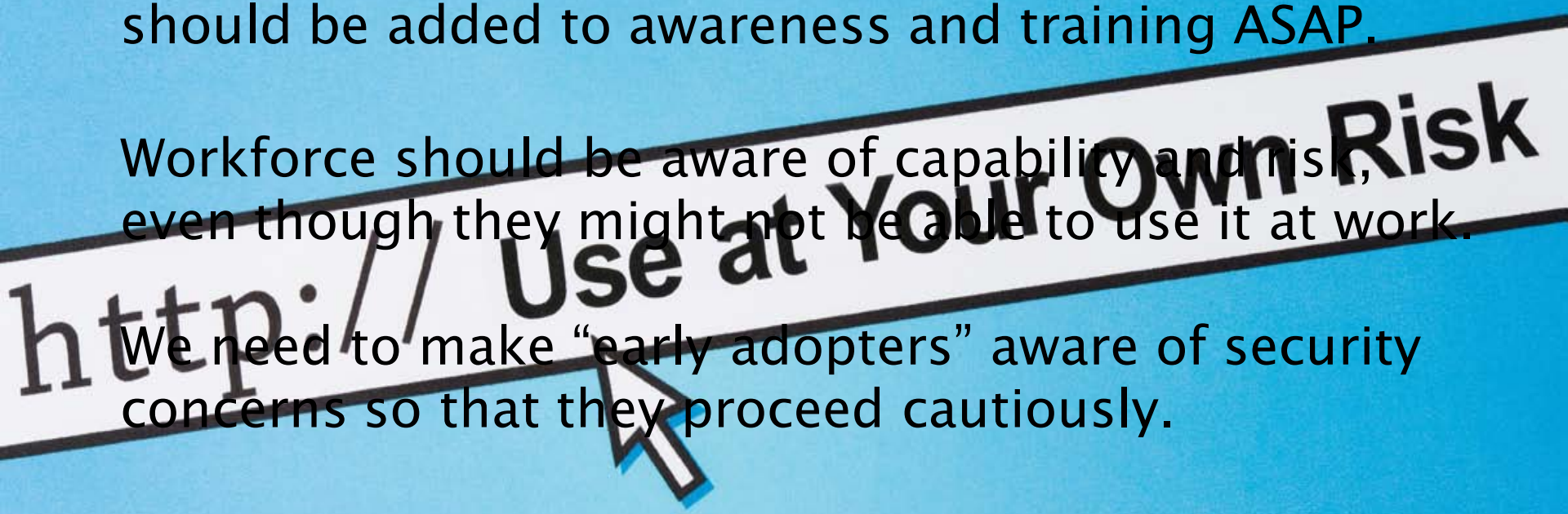
What should we do ?

New technologies and their business and personal use should be added to awareness and training ASAP.

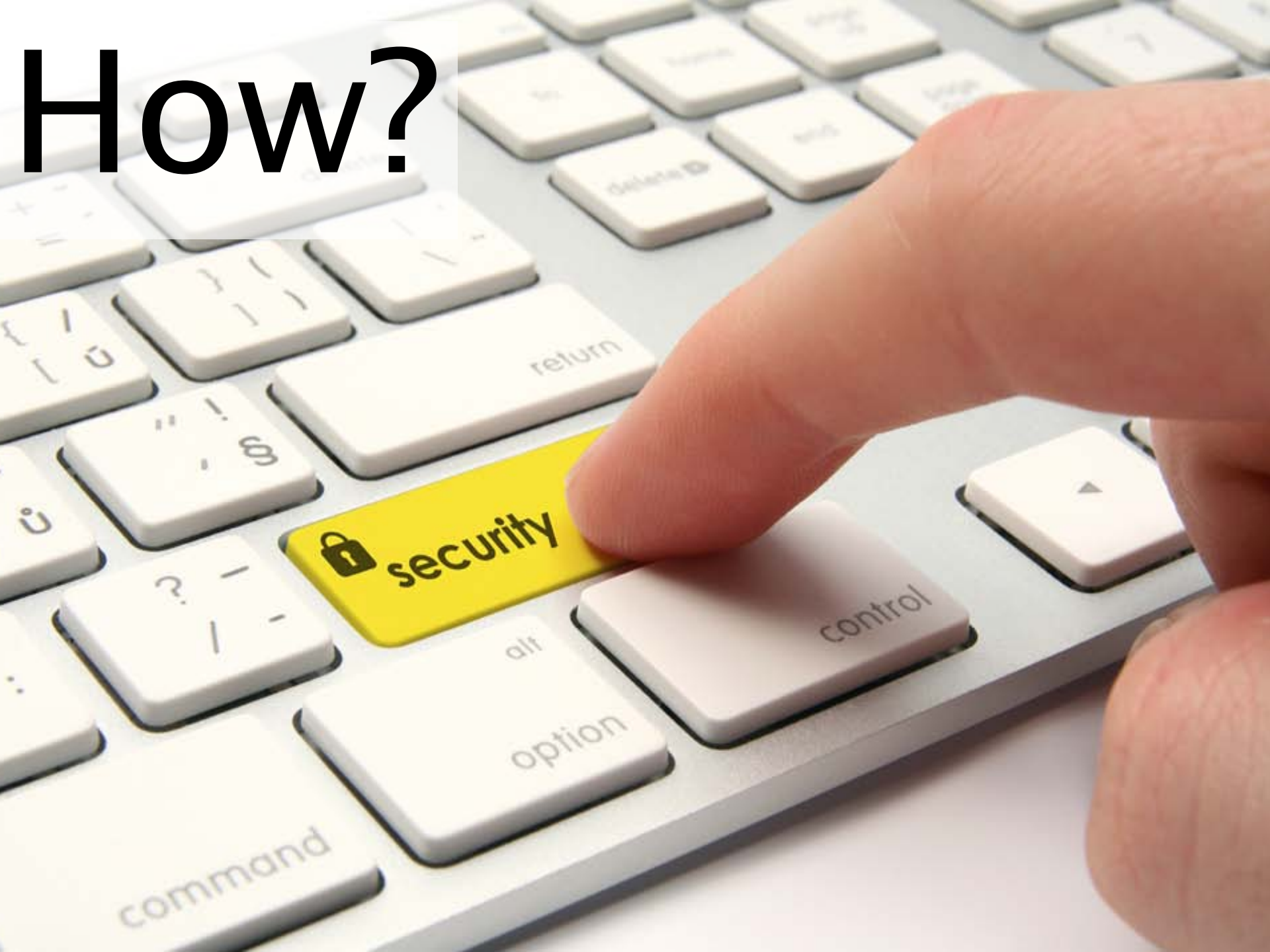
Workforce should be aware of capability and risk, even though they might not be able to use it at work.

We need to make “early adopters” aware of security concerns so that they proceed cautiously.

Workforce needs to be ready for the next attack, not the last.

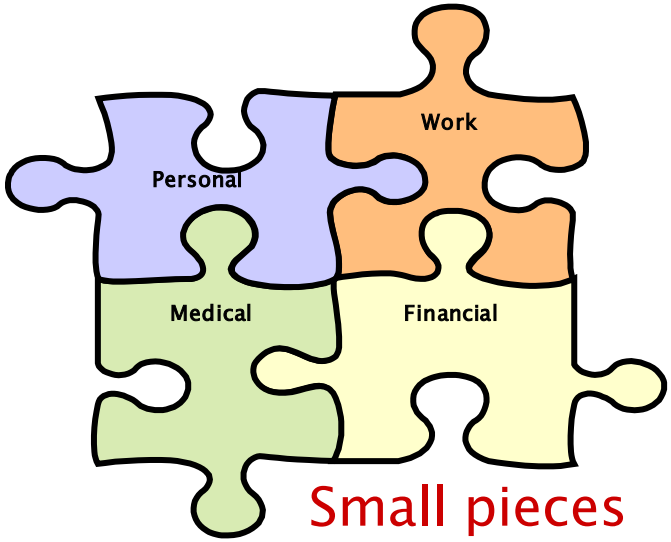


How?



User-Centered Awareness

- Security has value to the individual
- They lose control once data is published
  - Email addresses
  - Previous duty assignments
  - Photos of work locations
  - Job duties
  - Title, grade, or rank
  - Home and family photos
- Identify anything of value



Small pieces add up

Sanitize resumes, job boards

Every New Technology Has a Risk

- YouTube, 14.8 billion plus videos viewed in 2009
  - 50K views = front page
  - Viral distribution
- Manage Credit Card data
  - Credit services and AnnualCreditReport.com
- Pay Pal, Craig's List, eBay, and On Line purchases
- Twitter accounts $100-$200 per 1000
  - All twits go out with GPS location
  - No account information validation…who are you talking to?

Emphasize Simple Guidelines

- Don't assume someone else is responsible for security
- Shred everything….Everything
- Don't use your home mailbox
- Clean up your devices
- Reduce your electronic footprint
- You don't have to answer every question
- "Fight" the tendency to be friendly and to assume the best
  - What does the bad guy look like?
  - How do you know its him or her typing the message?

There are no SILVER Bullets to Security

Trust but Verify

Suggest Controls

- Home PC
  - Firewalls
  - Virus protection and anti-spyware -- auto scanning and updates On
  - Operating system up to date -- auto updates ON
  - Webcam OFF?
  - Internet Clear cache, cookies, history
  - Security setting – HIGH
  - Use trusted sites
  - Block pop ups
  - Control Active X
  - Be a user and not admin
  - Password at start up
  - File Sharing -- OFF
  - Once per week full system scan

How many virus protection packages do you need to protect your PC?

Suggest Controls

- Cell Phone
  - Password protect your phone
  - Lock your SIM card w/ a PIN
  - Delete personal information
  - Set GPS location only for 911
  - Disable remote connectivity
  - Disable your stolen phone
    - Get your serial number #06#
    - Write down the 15 digit code
    - Give the code to service provider
  - Use pre-paid phones for travel or sensitive calls
  - Emergency = 112 even when locked
  - Hidden Battery Power = *3370#

Every person on line is just another **STRANGER** on the street

Suggest Controls

- Blackberry (PDA)
  - All transmissions go through London and or Toronto
  - Encrypt your files
  - Password protect turn on
  - Set time out option
- Wireless and Bluetooth
  - Must be encrypted
  - Use in hidden mode. Can't be discovered
  - Don't use in public "hot spots"
  - Unencrypted sends all your information (psdws, email, & browsing)
- GPS
  - Don't use your "real" home address

Security is not a product

it is a never-ending story!

Suggest Controls

- Internet
  - Disable automated preview
  - Read email messages in plain text
  - Do not click on embedded links
  - Enter the web address directly
  - Do not open emails from unknown sources
  - Use PKI and tell others to
  - Use InPrivate, Incognito, or Private browsing – not perfect, but removes some “footprints”

The Internet was designed for survivability and for sharing

educational, research, & technical information,

however, it has become the “only” method of communication

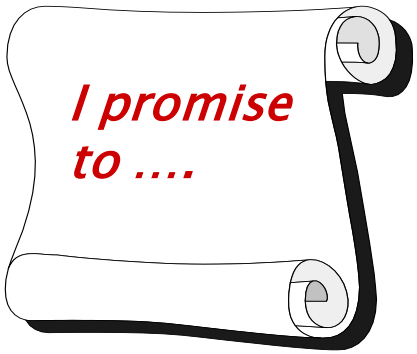
Suggest Controls

- Facebook Risk
  - 3rd parties applications
  - 500 million users and counting
  - 13 billion pictures
  - 46% of users accept friend requests from strangers
  - 89% of users in their 20's divulge their full birthday
  - 30-40% of users list data about family and friends.
  - 23% did not know there are privacy settings
  - Facebook Id's (email & pswd) = $25 per 1000 w/ 10 friends or less and $45 for 10 friends or more

Read the privacy guide and Disable all then turn on 1 by 1

Suggest Controls

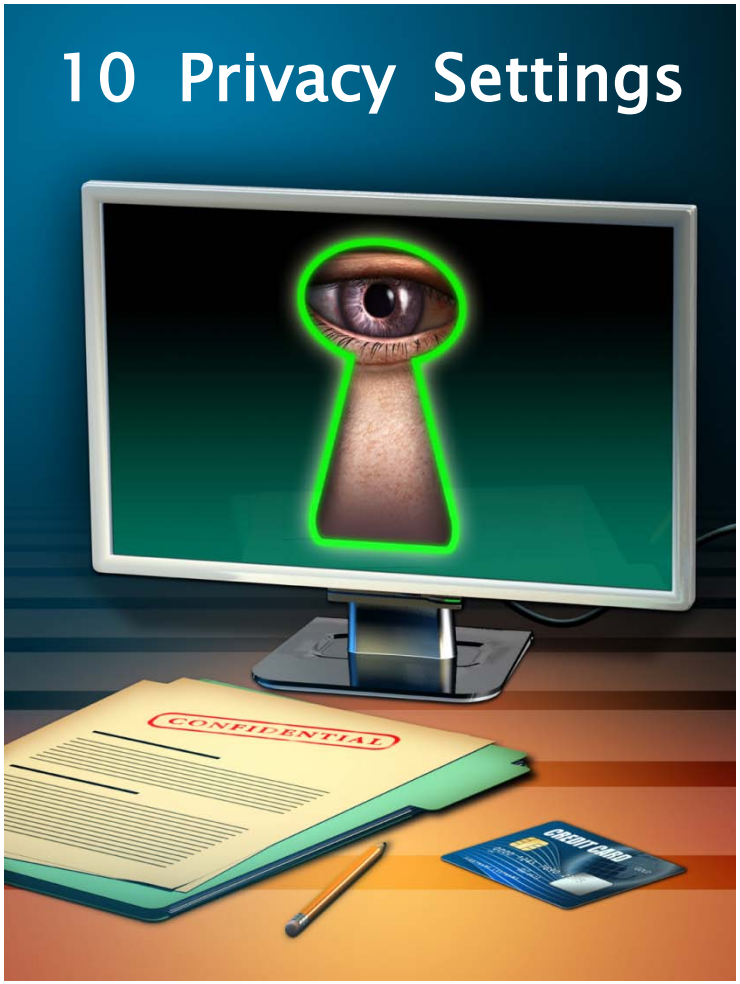
- Facebook Safety
  - Sign a contract with your friends



  - Settings and Privacy
    - What is your profile and search visibility?
    - Sort “friends” into groups and networks with different permissions
    - Validate a friend is really a friend. Call them!
    - Create untrusted group with lowest permissions and accesses

You are only as secure as your next friend

Suggest Controls



- Facebook Safety
  - Use friends lists
  - Avoid Photo/Video tags
  - Protect your Albums
  - Remove relationship status
  - Restrict Published Stories
  - Contact information private
  - Stop embarrassing wall posts
  - Friendships should be private
  - Remove yourself from Facebook Searches
  - Remove from Google searches

7/27/10 program looking for privacy settings enabling a public search = 171 million profiles

Suggest Controls

- Twitter
  - Don’t click on tiny urls
  - TwitWipe
- WhitePages.com, edit your information
- Google yourself at least once a year
  - Anonymity is good
  - Controlled dissemination is better
- Zabasearch.com, BeenVerified.com, and PublicRecords.com
- Review credit reports, bank, and credit card statements…line by line! (3 free per year)
- Credit cards, carry only what you need
- Don’t confirm anything to anyone over the phone

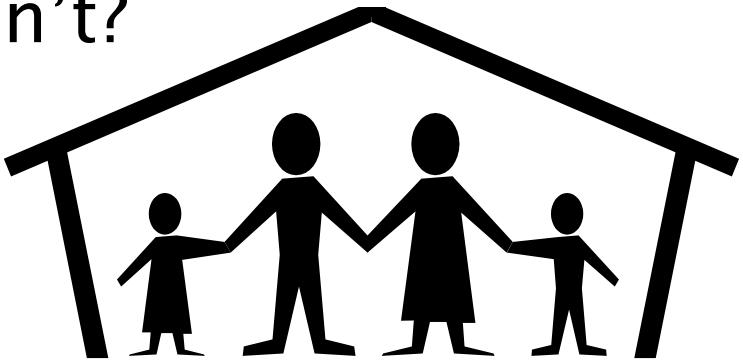
Suggest Controls

- Travel
  - Don't check devices unless you don't mind getting parts back
  - Don't lose sight of devices when being screened
  - Downsize to critical applications (anything you can afford to lose)
  - Don't "trust" anyone, your hotel or their safe
  - Beware of customs and other checkpoints
  - Remove the hard drive, or SIM card or disable the device
  - Use encryption, strong passwords, and change them often
  - Treat any network (hotel, cyber café, airport) as untrusted
  - Do not advertise your itinerary – or use your home address
  - Remember where you plugged in your converters

How do you make your cell phone safe?

Emphasize 3Security Questions

1. What are you sharing?
2. What are they going to do with your information and of what value is that to you?
3. How will they protect your information and what happens if they don't?



So, why are you online?

Resources

- US Cert, http://www.us-cert.gov/
- SNS Usage Checklist, https://www.iad.gov/ioss/index.cfm
- i-SAFE, http://www.isafe.org/
- OnGuardOnline, http://www.onguardonline.gov/
- All About Facebook
  http://www.allfacebook.com/facebook-privacy-2009-02
- Facebook Privacy
  http://socialmediasecurity.com/downloads/Facebook_Privacy_and_Security_Guide.pdf
- Social Networking
  http://theharmonyguy.com/
  http://www.social-engineer.org/se-resources/

Dr. Paul Krasley, paul.krasley@dia.mil, 703-907-2726

John Ippolito, John.Ippolito@Alliedtech.com – 301-309-1234