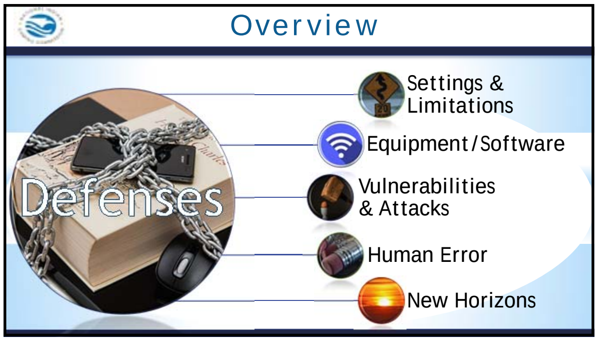
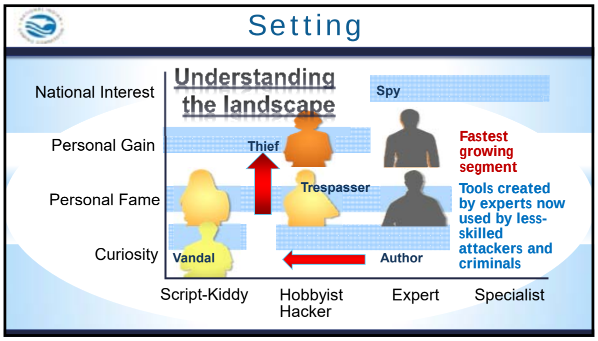
IT Vulnerabilities, Tech Exploits, and Cyber Defenses

Information Technology Division



Overview

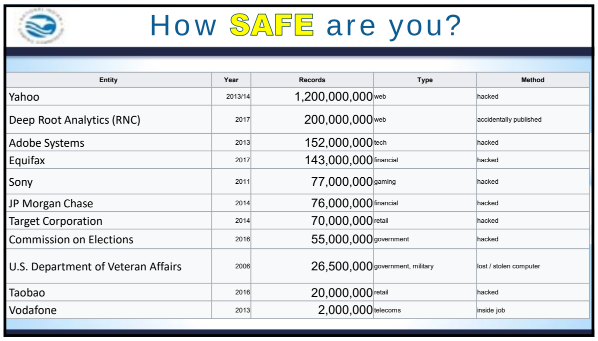
- Settings & Limitations
- Equipment/Software
- Vulnerabilities & Attacks
- Human Error
- New Horizons



Setting

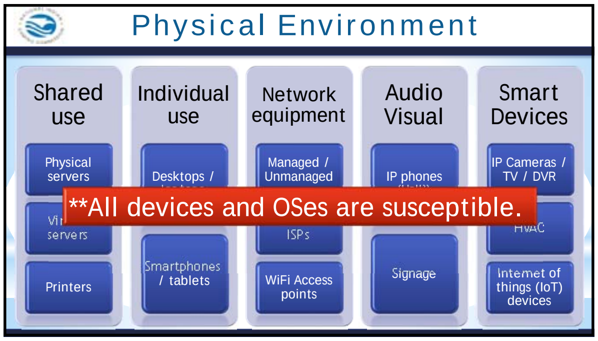
Fastest growing segment

Tools created by experts now used by less-skilled attackers and criminals



How SAFE are you?

Entity	Year	Records	Type	Method
Yahoo	2013/14	1,200,000,000	web	hacked
Deep Root Analytics (RNC)	2017	200,000,000	web	accidentally published
Adobe Systems	2013	152,000,000	tech	hacked
Equifax	2017	143,000,000	financial	hacked
Sony	2011	77,000,000	gaming	hacked
JP Morgan Chase	2014	76,000,000	financial	hacked
Target Corporation	2014	70,000,000	retail	hacked
Commission on Elections	2016	55,000,000	government	hacked
U.S. Department of Veteran Affairs	2006	26,500,000	government, military	lost / stolen computer
Taobao	2016	20,000,000	retail	hacked
Vodafone	2013	2,000,000	telecoms	inside job



Physical Environment

Shared use
- Physical servers
- Vi servers
- Printers

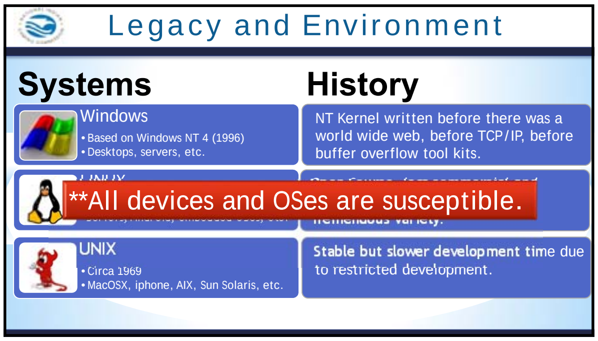
Individual use
- Desktops /
- Smartphones / tablets

Network equipment
- Managed / Unmanaged
- ISPs
- WiFi Access points

Audio Visual
- IP phones
- Signage

Smart Devices
- IP Cameras / TV / DVR
- HVAC
- Internet of things (IoT) devices

**All devices and OSes are susceptible.



Legacy and Environment

Systems

Windows
- Based on Windows NT 4 (1996)
- Desktops, servers, etc.

LINUX

UNIX
- Circa 1969
- MacOSX, iphone, AIX, Sun Solaris, etc.

History

NT Kernel written before there was a world wide web, before TCP/IP, before buffer overflow tool kits.

tremendous variety.

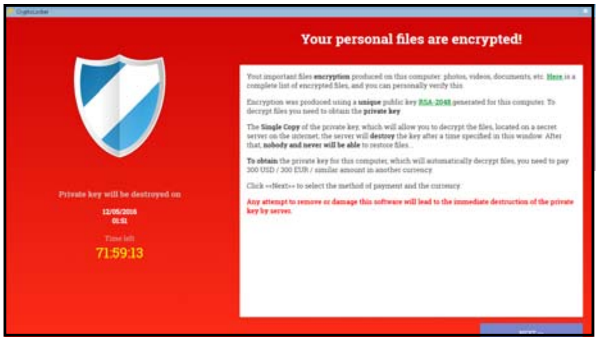
Stable but slower development time due to restricted development.

**All devices and OSes are susceptible.

Attacks, Tools and Terminology

Zero-day Vulnerability

They are known as 0-day vulnerabilities, because there are zero days to create a patch. They are unknown to authors and unprotected by anti-virus / anti-malware software.



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key**.

The **Single Copy** of the private key, which will allow you to decrypt the files, located on a secret server on the internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay 300 USD / 300 EUR / similar amount in another currency.

Click <<Next>> to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on

12/05/2016
01:51

Time left

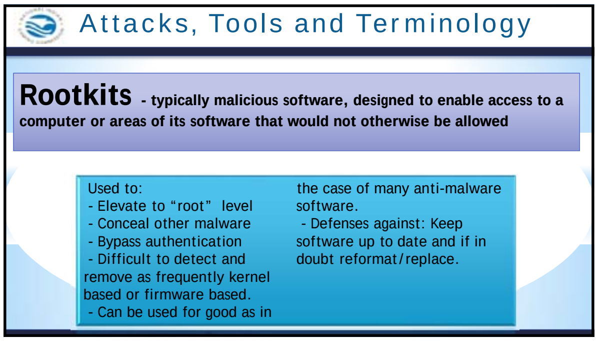
71:59:13

Attacks, Tools and Terminology

Denial of Service (DoS)

- Denial of Service or (DoS) or Distributed Denial of Service Attacks (DDoS)
- Deny service to the intended machine or network resource
- Can originate from multiple sources
- Made famous by "hacktivists"
- Defenses?

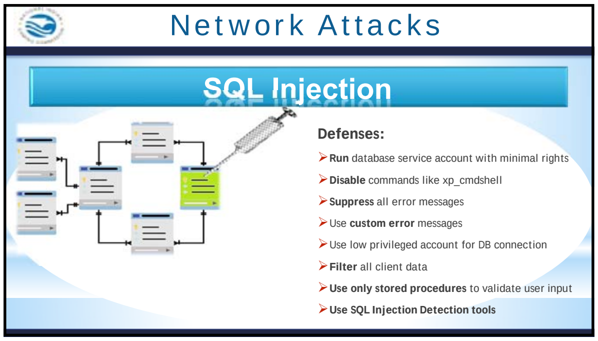
**2017 WannaCry DDoS attack affected IIS on legacy XP and 2003 systems



Attacks, Tools and Terminology

Rootkits - **typically malicious software, designed to enable access to a computer or areas of its software that would not otherwise be allowed**

Used to:
- Elevate to "root" level
- Conceal other malware
- Bypass authentication
- Difficult to detect and remove as frequently kernel based or firmware based.
- Can be used for good as in the case of many anti-malware software.
- Defenses against: Keep software up to date and if in doubt reformat/replace.

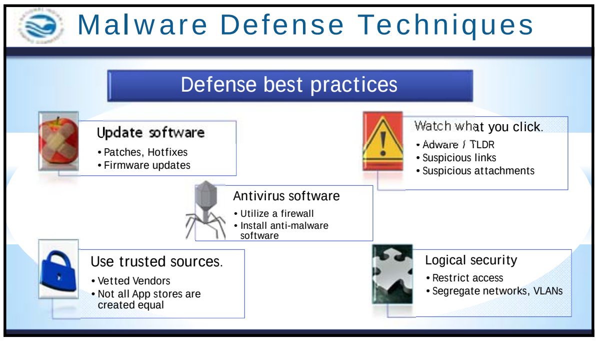


Network Attacks

SQL Injection

Defenses:

- **Run** database service account with minimal rights
- **Disable** commands like xp_cmdshell
- **Suppress** all error messages
- Use **custom error** messages
- Use low privileged account for DB connection
- **Filter** all client data
- **Use only stored procedures** to validate user input
- **Use SQL Injection Detection tools**



Malware Defense Techniques

Defense best practices

Update software
- Patches, Hotfixes
- Firmware updates

Watch what you click.
- Adware / TLDR
- Suspicious links
- Suspicious attachments

Antivirus software
- Utilize a firewall
- Install anti-malware software

Use trusted sources.
- Vetted Vendors
- Not all App stores are created equal

Logical security
- Restrict access
- Segregate networks, VLANs

Activity – Identify the Dangers

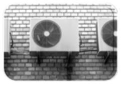
Smart TVs

IP cameras

VoIP phones

Printers

Voice recognition
software


HVAC

Cable / Satellite

POS

Wireless Network Attacks

Packet Sniffing / AP impersonation

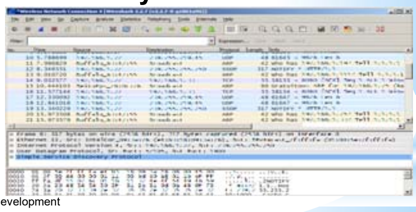
❖**Types of attacks**:

- ➢DHCP Attacks
- ➢ARP Poisoning
- ➢Spoofing / Evil Twin
- ➢DNS Poisoning
- ➢Password Capture
- ➢Wireless pivots

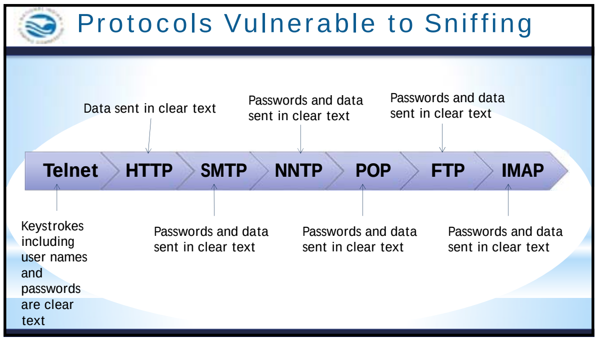
Network Hacking Tools

Packet Analyzers

- ➢ Troubleshooting
- ➢ Analysis
- ➢ Software development
- ➢ Education
- ➢ Sees all traffic
- ➢ Graphical front-end
- ➢ Can sort and & filter
- ➢ Communications protocol development
- ➢ Puts network interface into promiscuous mode



Activity – Wireshark Demo



Protocols Vulnerable to Sniffing

Telnet: Keystrokes including user names and passwords are clear text

HTTP: Data sent in clear text

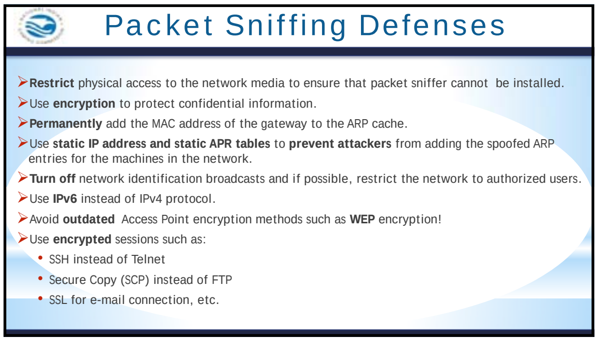
SMTP: Passwords and data sent in clear text

NNTP: Passwords and data sent in clear text

POP: Passwords and data sent in clear text

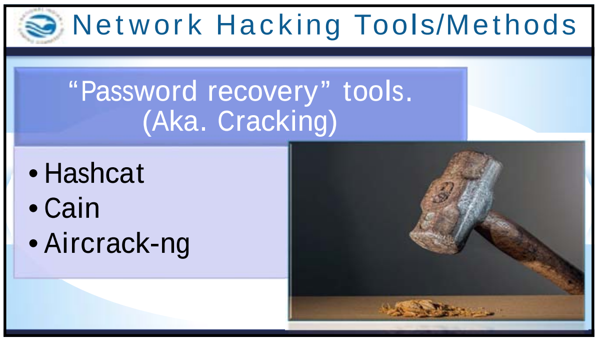
FTP: Passwords and data sent in clear text

IMAP: Passwords and data sent in clear text



Packet Sniffing Defenses

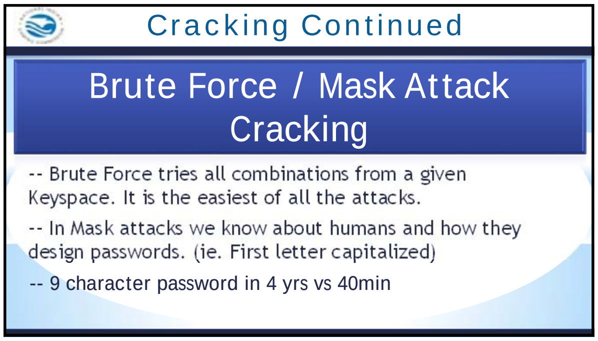
- **Restrict** physical access to the network media to ensure that packet sniffer cannot be installed.
- Use **encryption** to protect confidential information.
- **Permanently** add the MAC address of the gateway to the ARP cache.
- Use **static IP address and static APR tables** to **prevent attackers** from adding the spoofed ARP entries for the machines in the network.
- **Turn off** network identification broadcasts and if possible, restrict the network to authorized users.
- Use **IPv6** instead of IPv4 protocol.
- Avoid **outdated** Access Point encryption methods such as **WEP** encryption!
- Use **encrypted** sessions such as:
  - SSH instead of Telnet
  - Secure Copy (SCP) instead of FTP
  - SSL for e-mail connection, etc.



Network Hacking Tools/Methods

"Password recovery" tools.
(Aka. Cracking)

- Hashcat
- Cain
- Aircrack-ng



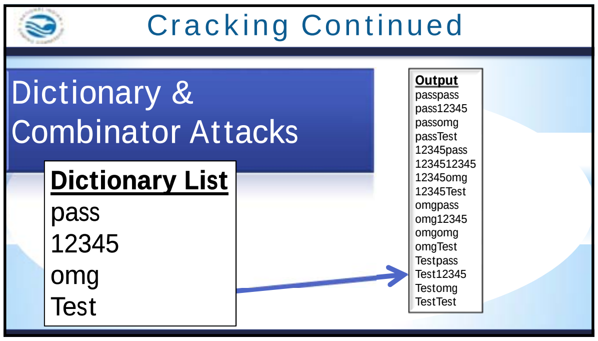
Cracking Continued

Brute Force / Mask Attack Cracking

-- Brute Force tries all combinations from a given Keyspace. It is the easiest of all the attacks.

-- In Mask attacks we know about humans and how they design passwords. (ie. First letter capitalized)

-- 9 character password in 4 yrs vs 40min



Cracking Continued

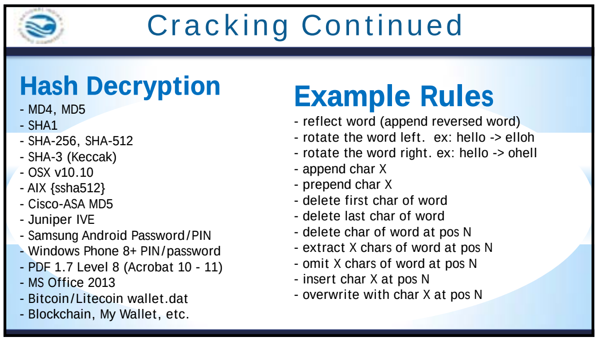
Dictionary & Combinator Attacks

Dictionary List

pass
12345
omg
Test

Output

passpass
pass12345
passomg
passTest
12345pass
1234512345
12345omg
12345Test
omgpass
omg12345
omgomg
omgTest
Testpass
Test12345
Testomg
TestTest



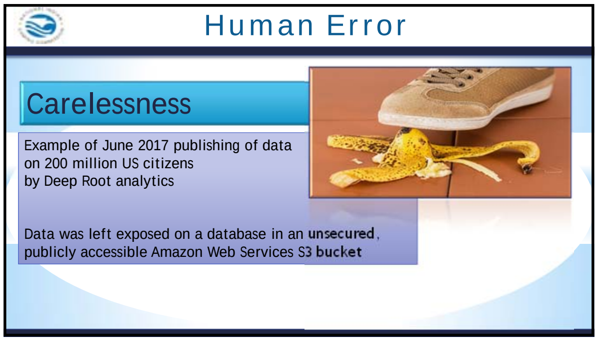
Cracking Continued

Hash Decryption

- MD4, MD5
- SHA1
- SHA-256, SHA-512
- SHA-3 (Keccak)
- OSX v10.10
- AIX {ssha512}
- Cisco-ASA MD5
- Juniper IVE
- Samsung Android Password/PIN
- Windows Phone 8+ PIN/password
- PDF 1.7 Level 8 (Acrobat 10 - 11)
- MS Office 2013
- Bitcoin/Litecoin wallet.dat
- Blockchain, My Wallet, etc.

Example Rules

- reflect word (append reversed word)
- rotate the word left. ex: hello -> elloh
- rotate the word right. ex: hello -> ohell
- append char X
- prepend char X
- delete first char of word
- delete last char of word
- delete char of word at pos N
- extract X chars of word at pos N
- omit X chars of word at pos N
- insert char X at pos N
- overwrite with char X at pos N

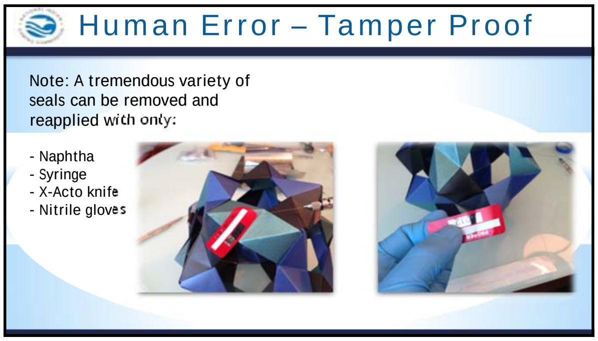


Human Error

Carelessness

Example of June 2017 publishing of data on 200 million US citizens by Deep Root analytics

Data was left exposed on a database in an **unsecured**, publicly accessible Amazon Web Services S3 **bucket**



Human Error – Tamper Proof

Note: A tremendous variety of seals can be removed and reapplied with only:

- Naphtha
- Syringe
- X-Acto knife
- Nitrile gloves

Human Error–Social Engineering

The art of convincing people to reveal confidential information.

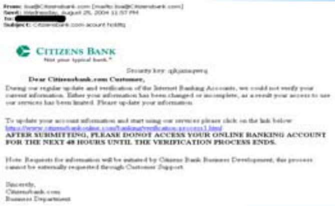
Phases in a Social Engineering Attack

- **Research Target Company**
  Dumpster diving, websites, employees, tour company, etc.
- **Select Victim**
  Identify a frustrated employee
- **Develop Relationship**
  Build some type of personal relationship with the selected employee
- **Exploit**
  Collect sensitive personal information (kids' names, birthdays), financial information or current company technologies

Human Error–Social Engineering

Phishing

- Designed to fraudulently obtain private information
- Generally, does not involve personal contact, usually legitimate looking E-mail, websites, or other electronic means are involved in phishing attacks. (ie. QR codes. USB thumb drives, etc)



From: lsa@Citizensbank.com [mailto:lsa@Citizensbank.com]
Sent: Wednesday, August 25, 2004 11:57 PM
To: [redacted]
Subject: Citizensbank.com acount holdg

CITIZENS BANK
Not your typical bank.®

Security key: qjkjasuqwrq

Dear Citizensbank.com Customer,

During our regular update and verification of the Internet Banking Accounts, we could not verify your current information. Either your information has been changed or incomplete, as a result your access to use our services has been limited. Please up-date your information.

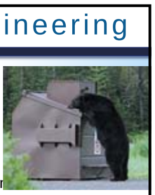
To update your account information and start using our services please click on the link below:
https://www.citizensbankonline.com/banking/verification-process1.html
AFTER SUBMITTING, PLEASE DONOT ACCESS YOUR ONLINE BANKING ACCOUNT FOR THE NEXT 48 HOURS UNTIL THE VERIFICATION PROCESS ENDS.

Note: Requests for information will be initiated by Citizens Bank Business Development, this process cannot be externally requested through Customer Support.

Sincerely,
Citizensbank.com
Business Department

Human Error–Social Engineering

Dumpster Diving / Trashing



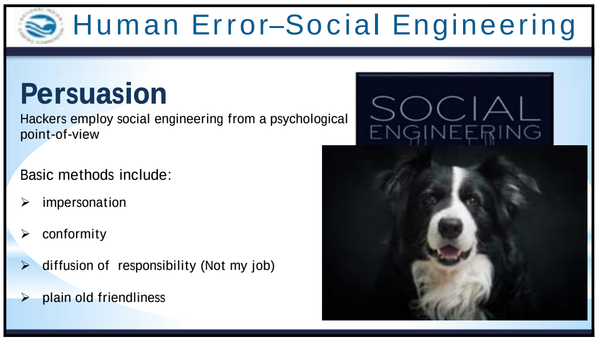
Large amounts of information can be collected through company trash, such as:

company phone books - organizational charts - memos - system m

calendars of meetings - events and vacations - company policy manuals

printouts of sensitive data or login names and passwords - printouts of source code

disks and tapes - company letterhead and memo forms - outdated hardware



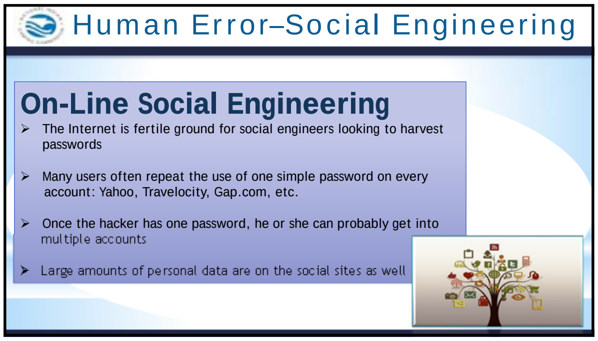
Human Error–Social Engineering

Persuasion

Hackers employ social engineering from a psychological point-of-view

Basic methods include:

- impersonation
- conformity
- diffusion of responsibility (Not my job)
- plain old friendliness



Human Error–Social Engineering

On-Line Social Engineering

- The Internet is fertile ground for social engineers looking to harvest passwords
- Many users often repeat the use of one simple password on every account: Yahoo, Travelocity, Gap.com, etc.
- Once the hacker has one password, he or she can probably get into multiple accounts
- Large amounts of personal data are on the social sites as well

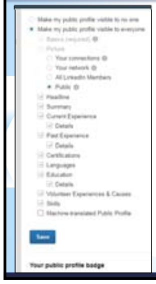
SOCIAL
MEDIA

Human Error – Social Media

Tips for securing your online profile

> Carefully choose your audience.
(Friends, friends of friends, public)
> Use a Secret Email Address
> Secure Those Security Questions
> Set Up Login Notifications (dual factor auth)
> Don’t link accounts

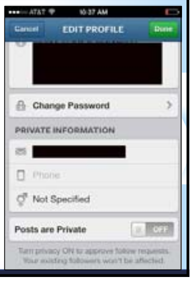
Activity – Identify the Problem(s)



○ Make my public profile visible to no one
● Make my public profile visible to everyone
☑ Basics (required)
☑ Picture
○ Your connections
○ Your network
○ All LinkedIn Members
● Public
☑ Headline
☑ Summary
☑ Current Experience
☑ Details
☑ Past Experience
☑ Details
☑ Certifications
☑ Languages
☑ Education
☑ Details
☑ Volunteer Experiences & Causes
☑ Skills
□ Machine-translated Public Profile

Your public profile badge

What's wrong with these profile settings?



[redacted]

Change Password

PRIVATE INFORMATION

[redacted]

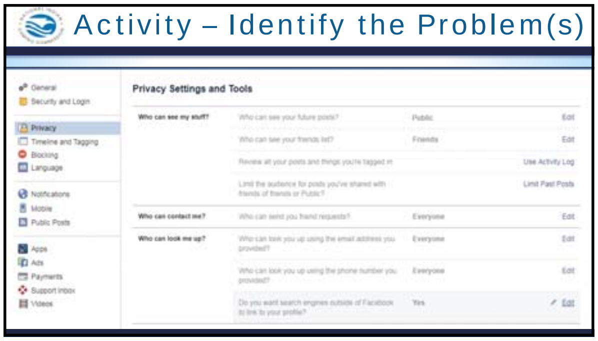
Phone

Not Specified

Posts are Private — OFF

Turn privacy ON to approve follow requests. Your existing followers won't be affected.

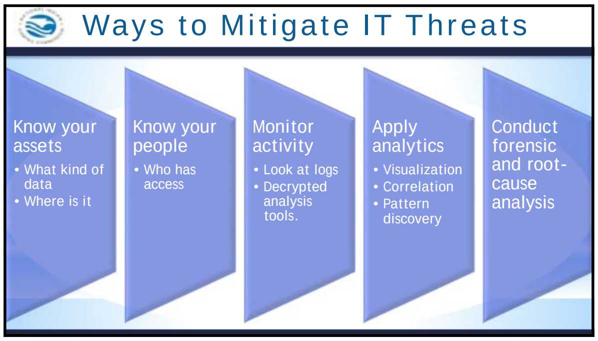
Activity – Identify the Problem(s)



Privacy Settings and Tools

Who can see my stuff?	Who can see your future posts?	Public	Edit
	Who can see your friends list?	Friends	Edit
	Review all your posts and things you're tagged in		Use Activity Log
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
Who can contact me?	Who can send you friend requests?	Everyone	Edit
Who can look me up?	Who can look you up using the email address you provided?	Everyone	Edit
	Who can look you up using the phone number you provided?	Everyone	Edit
	Do you want search engines outside of Facebook to link to your profile?	Yes	Edit

Ways to Mitigate IT Threats



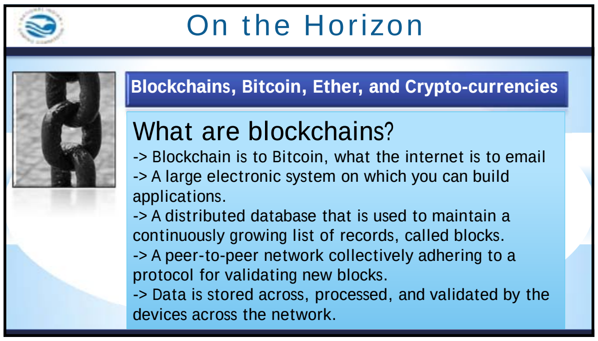
Know your assets
- What kind of data
- Where is it

Know your people
- Who has access

Monitor activity
- Look at logs
- Decrypted analysis tools.

Apply analytics
- Visualization
- Correlation
- Pattern discovery

Conduct forensic and root-cause analysis

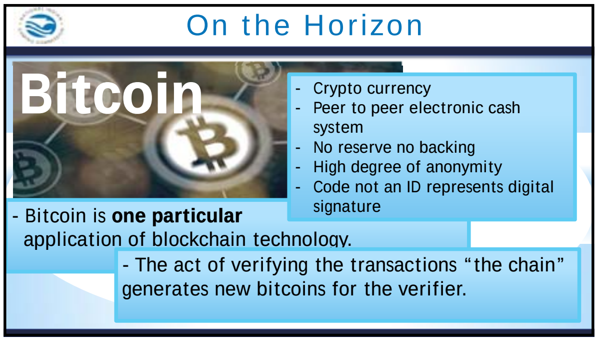


On the Horizon

Blockchains, Bitcoin, Ether, and Crypto-currencies

What are blockchains?

-> Blockchain is to Bitcoin, what the internet is to email
-> A large electronic system on which you can build applications.
-> A distributed database that is used to maintain a continuously growing list of records, called blocks.
-> A peer-to-peer network collectively adhering to a protocol for validating new blocks.
-> Data is stored across, processed, and validated by the devices across the network.

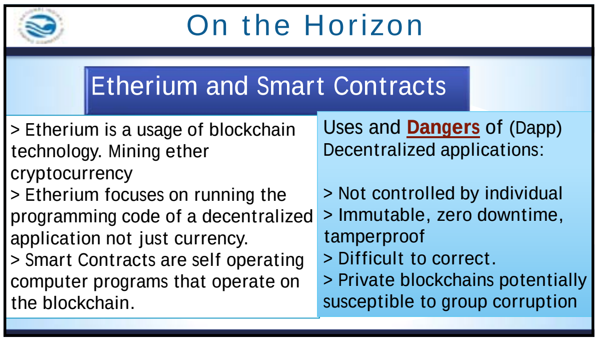


On the Horizon

- Crypto currency
- Peer to peer electronic cash system
- No reserve no backing
- High degree of anonymity
- Code not an ID represents digital signature

- Bitcoin is **one particular** application of blockchain technology.

- The act of verifying the transactions "the chain" generates new bitcoins for the verifier.



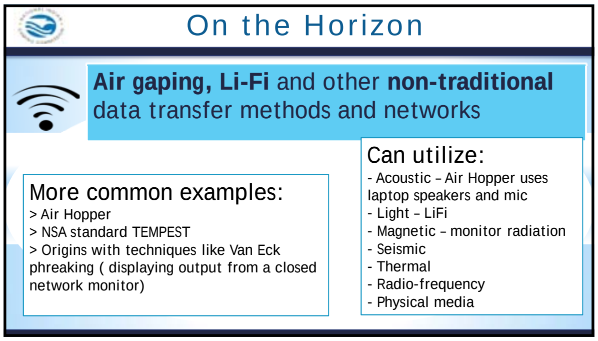
On the Horizon

Etherium and Smart Contracts

> Etherium is a usage of blockchain technology. Mining ether cryptocurrency
> Etherium focuses on running the programming code of a decentralized application not just currency.
> Smart Contracts are self operating computer programs that operate on the blockchain.

Uses and **Dangers** of (Dapp) Decentralized applications:

> Not controlled by individual
> Immutable, zero downtime, tamperproof
> Difficult to correct.
> Private blockchains potentially susceptible to group corruption



On the Horizon

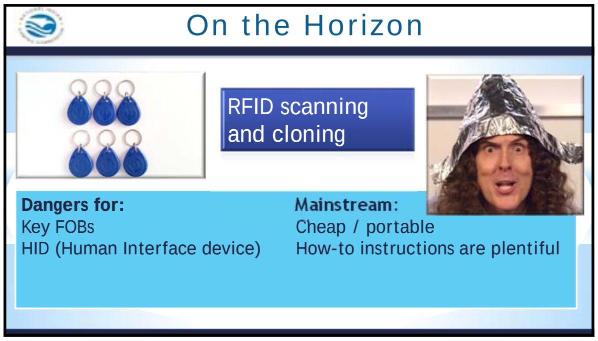
Air gaping, Li-Fi and other **non-traditional** data transfer methods and networks

More common examples:

> Air Hopper
> NSA standard TEMPEST
> Origins with techniques like Van Eck phreaking (displaying output from a closed network monitor)

Can utilize:

- Acoustic – Air Hopper uses laptop speakers and mic
- Light – LiFi
- Magnetic – monitor radiation
- Seismic
- Thermal
- Radio-frequency
- Physical media

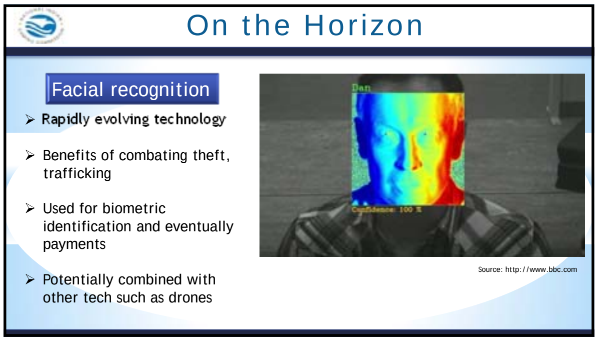


On the Horizon

RFID scanning and cloning

Dangers for:
Key FOBs
HID (Human Interface device)

Mainstream:
Cheap / portable
How-to instructions are plentiful



On the Horizon

Facial recognition

- Rapidly evolving technology
- Benefits of combating theft, trafficking
- Used for biometric identification and eventually payments
- Potentially combined with other tech such as drones

Dan
Confidence: 100 %

Source: http://www.bbc.com

On the Horizon

Honeypots http://map.norsecorp.com/#/

Questions

Tim Cotton
IT Auditor
timothy_cotton@nigc.gov

Jeran Cox
IT Auditor
jeran_cox@nigc.gov

Michael Curry
IT Auditor
michael_curry@nigc.gov

Sean Mason
IT Auditor
sean_mason@nigc.gov

Travis Waldo
Director, IT
travis_waldo@nigc.gov

Course Evaluation

- Provide an honest assessment of your experience
- Written suggestions and comments are greatly appreciated and allow us to improve your experience

Course Eval IT-108 IT Threats

When survey is active, respond at **PollEv.com/nigc**

Start the presentation to activate live content

If you see this message in presentation mode, install the add-in or get help at PollEv.com/app

0 surveys underway