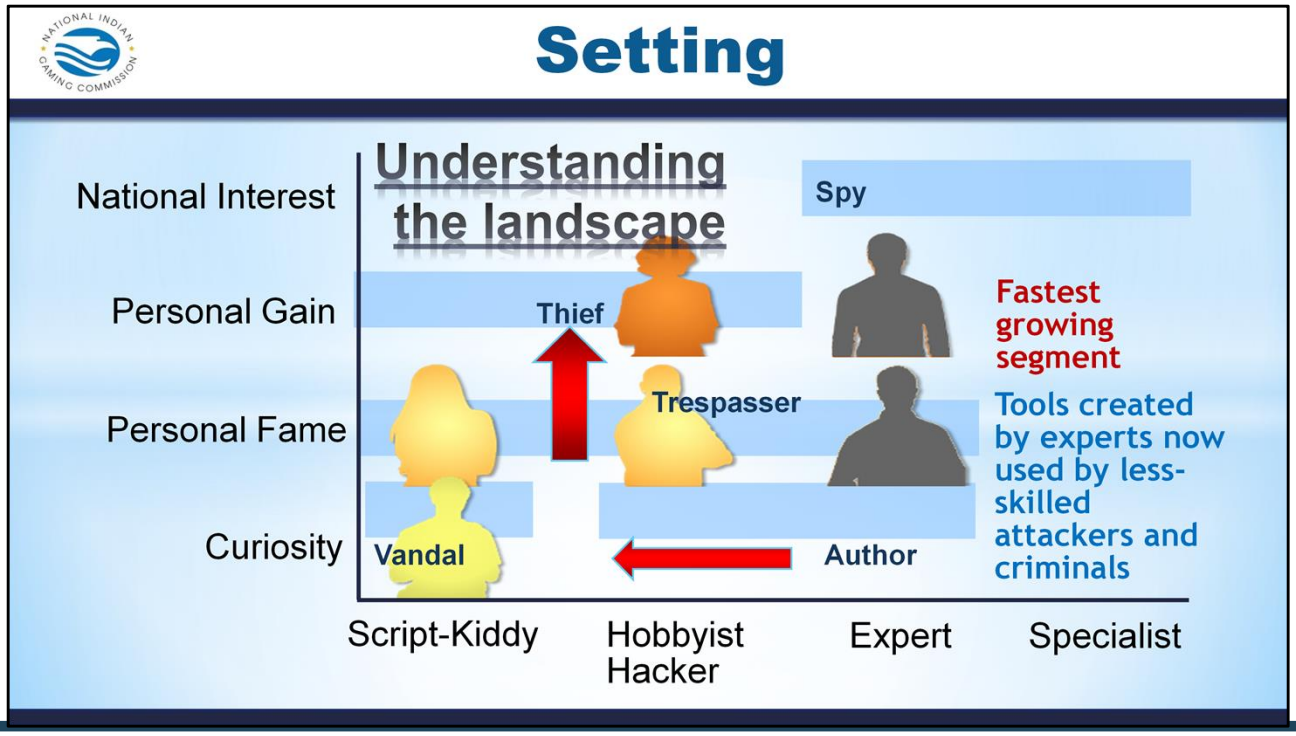
IT-108 IT Vulnerabilities, Tech Exploits, and Cyber Defenses

Information Technology Division

KEY POINTS


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

KEY POINTS



KEY POINTS

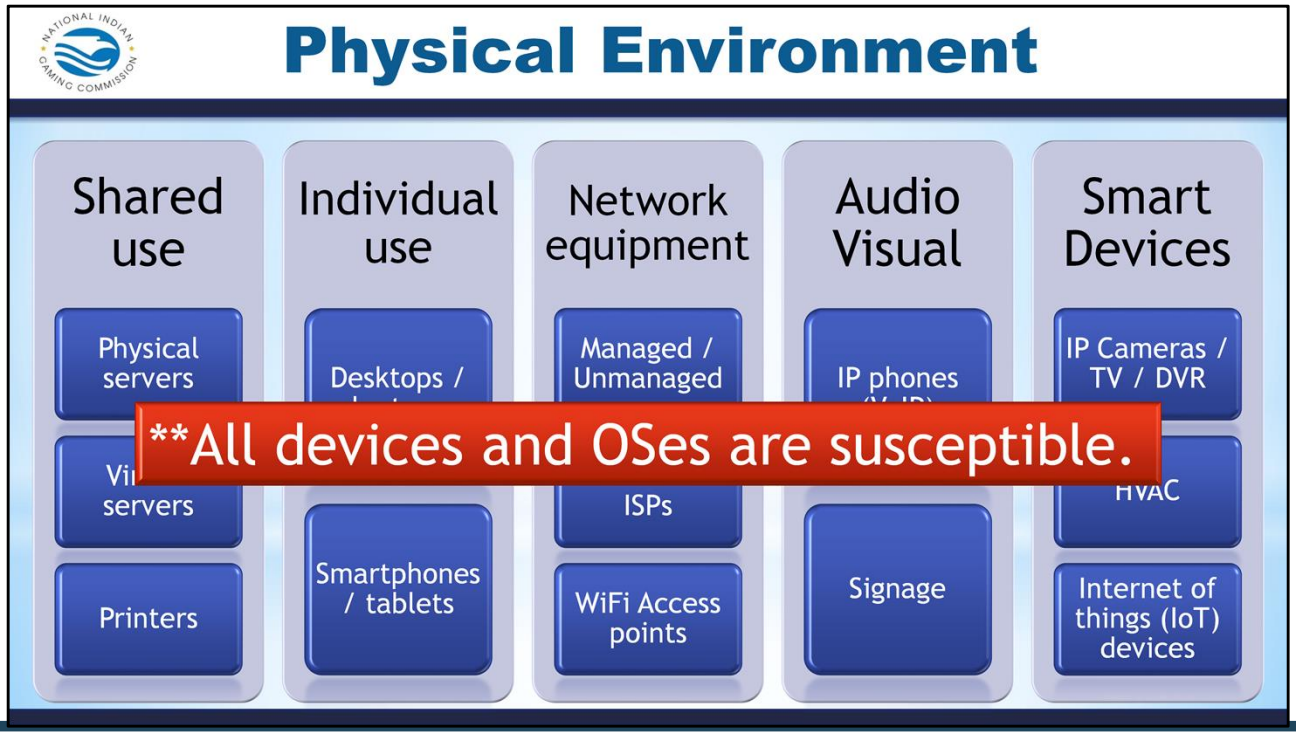
Types of attackers and reasons for attack:
Curiosity, Fame, Personal gain, National Interest
Script-Kiddy, Hobbyists, Experts, Specialist

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

KEY POINTS

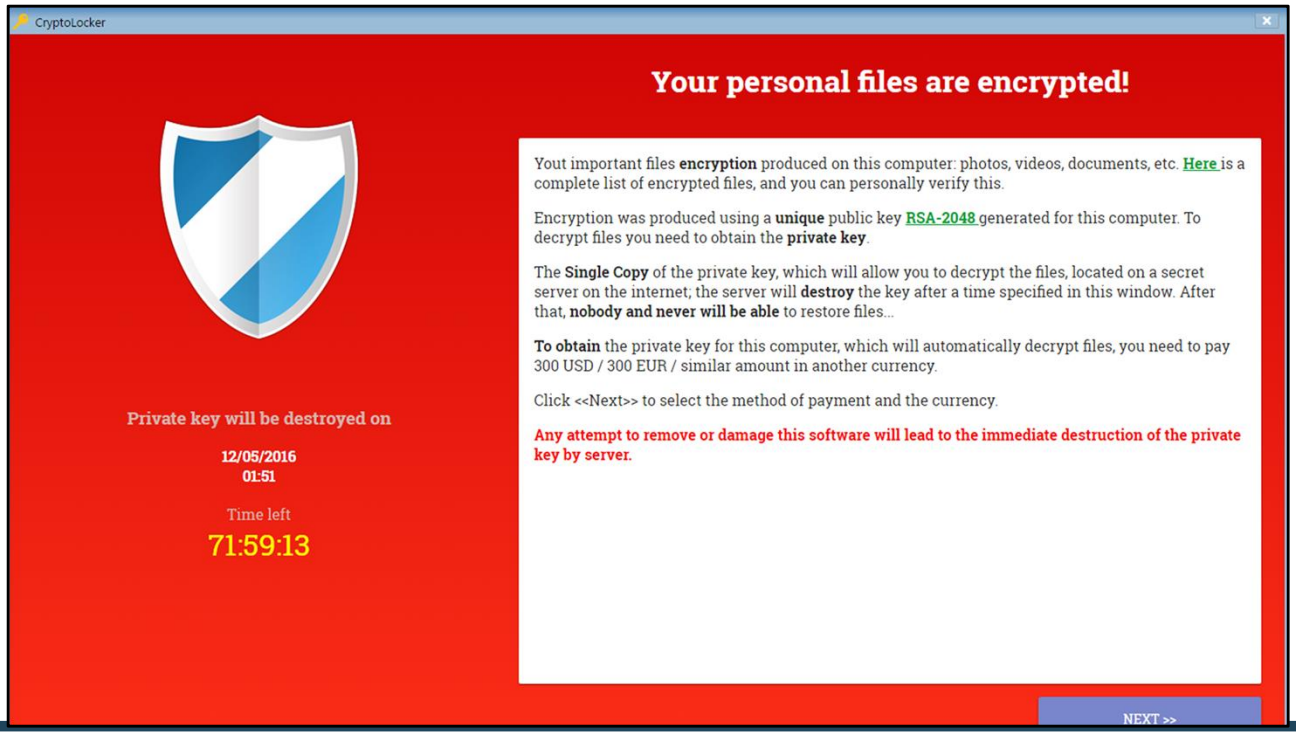
There are numerous ways that attacks and incidents can occur. Some malicious some accidental. No industry is safe.



KEY POINTS

There are numerous devices and systems types that have to be consideredwhen thinking about a casino's IT secuity. Each with it's own unique points of interest.

Remember no devices or Operating Systems is completely secure



KEY POINTS

CryptoLockers are a type of Ransomware.

Remember to perform daily backups of critical systems.

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

KEY POINTS

Not all types of attacks are to steal money or data. Sometimes disruption is the goal. DoS attacks fall under that category.


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

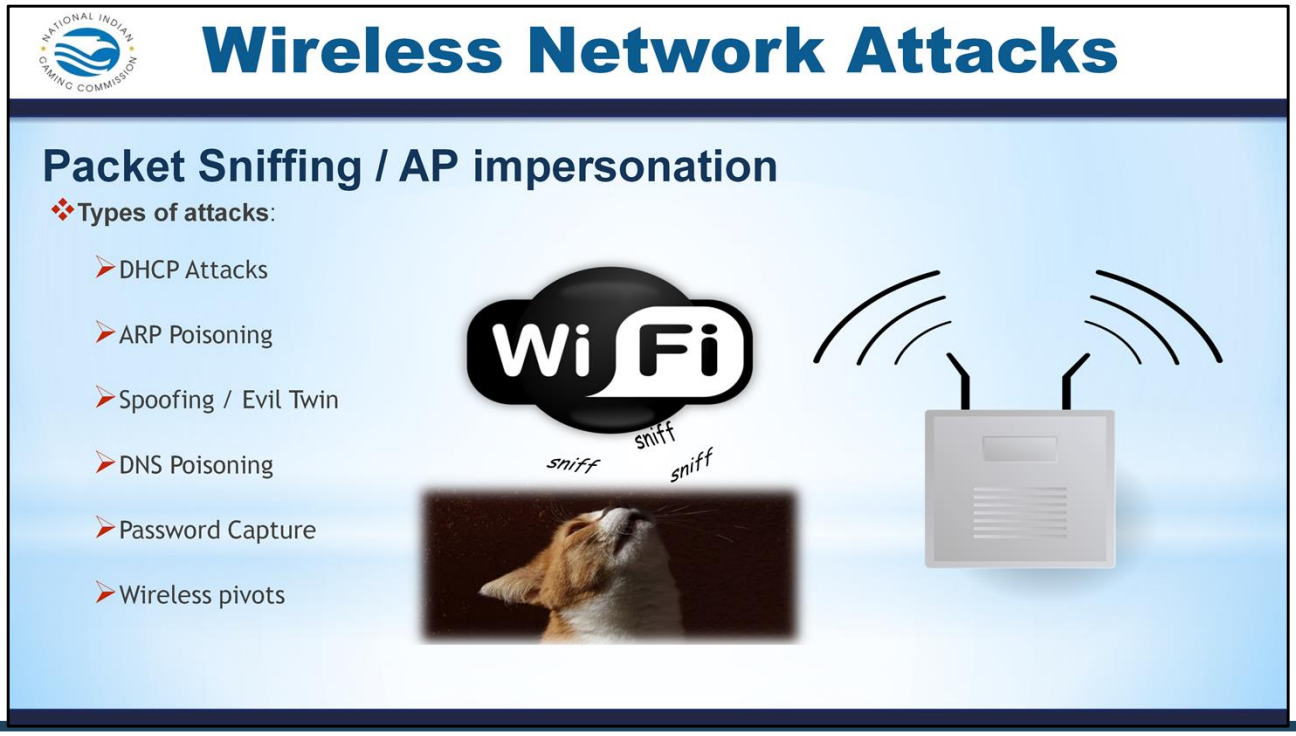
KEY POINTS

KEY POINTS

Activity:

Break into groups. Discuss in groups the types of dangers with each family of systems.

* Remember not all IT vulnerabilities involve a personal computer.



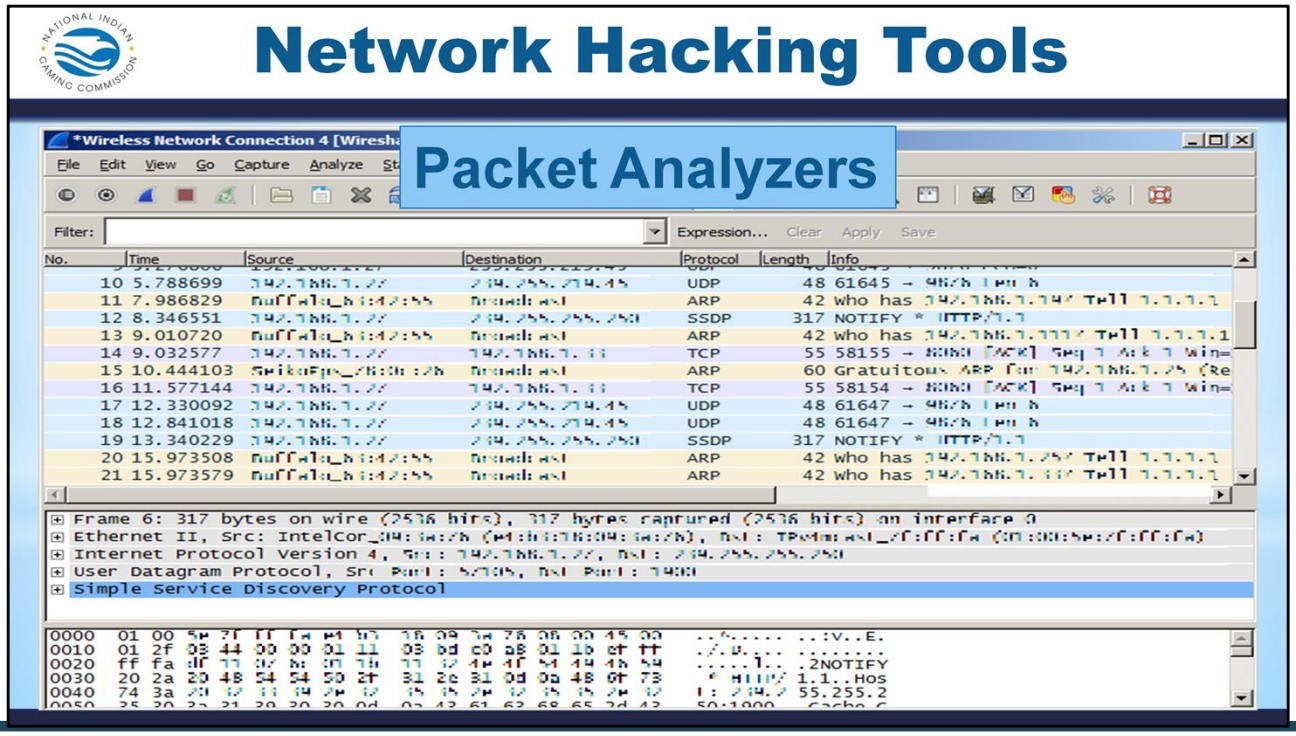
KEY POINTS

A variety of attacks and vulnerabilities exist.

Not all encryption methods are created equally.

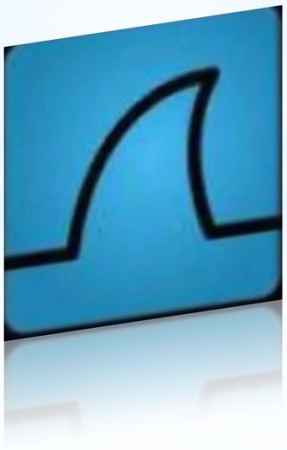
(ie. WPA2-EAP-TLS >> WPA2-EAP-PEAP/EAPTTLS. >> WEP2)

*When possible have a system with separate authenticator and authentication server.

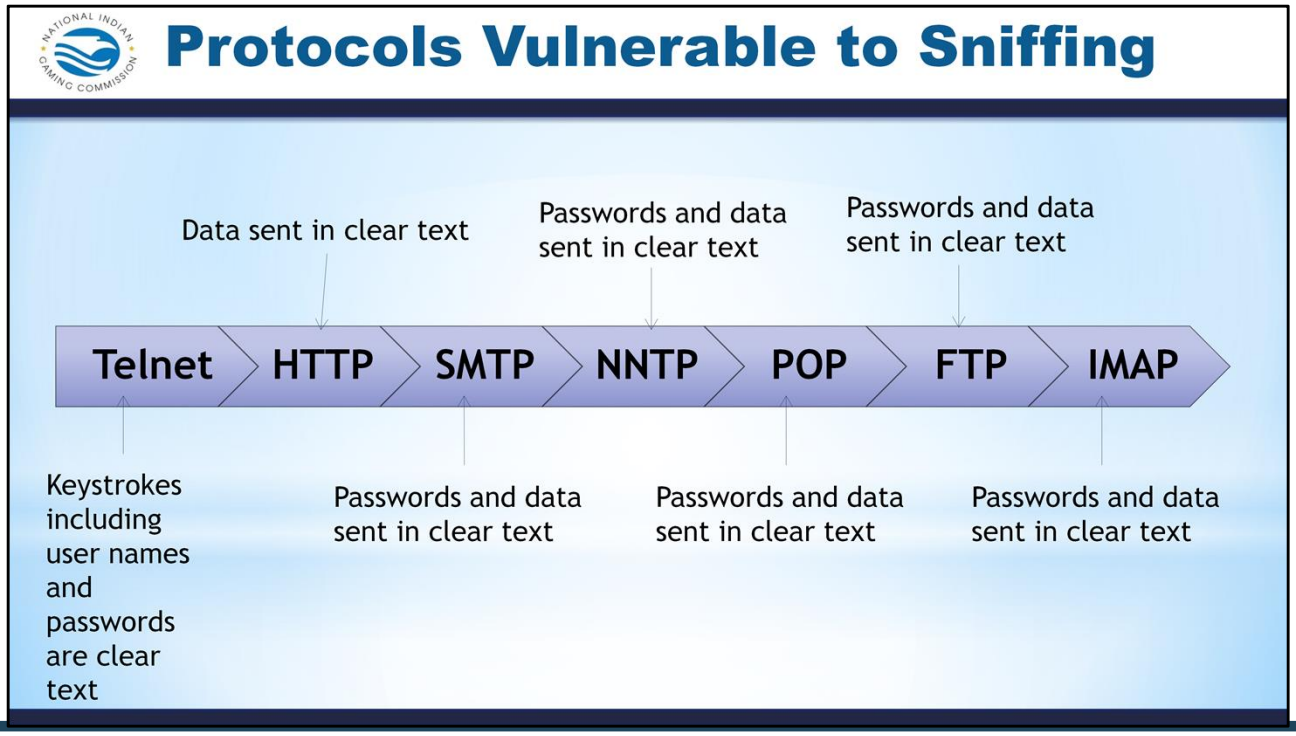

Network Hacking Tools
Packet Analyzers
*Wireless Network Connection 4 [Wiresh
File Edit View Go Capture Analyze
Filter:
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
10 5.788699 UDP 48 61645 → 9626 Len=6
11 7.986829 ARP 42 who has 192.168.1.192 Tell 1.1.1.1
12 8.346551 SSDP 317 NOTIFY * HTTP/1.1
13 9.010720 ARP 42 who has 192.168.1.1111 Tell 1.1.1.1
14 9.032577 TCP 55 58155 → 8000 [ACK] Seq=1 Ack=1 Win=
15 10.444103 ARP 60 Gratuitous ARP for 192.168.1.25 (Re
16 11.577144 TCP 55 58154 → 8000 [ACK] Seq=1 Ack=1 Win=
17 12.330092 UDP 48 61647 → 9626 Len=6
18 12.841018 UDP 48 61647 → 9626 Len=6
19 13.340229 SSDP 317 NOTIFY * HTTP/1.1
20 15.973508 ARP 42 who has 192.168.1.252 Tell 1.1.1.1
21 15.973579 ARP 42 who has Tell 1.1.1.1
Frame 6: 317 bytes on wire (2536 bits), 317 bytes captured (2536 bits) on interface 0
Ethernet II, Src: IntelCor_04:1a:26
Internet Protocol Version 4, Src: 192.168.1.22, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 57105, Dst Port: 1900
Simple Service Discovery Protocol
0000 01 00 5e 7f ff fa
0010 01 2f 03 44 00 00 01 11
0020 ff fa
0030 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73
0040 74 3a
..:V..E.
.2NOTIFY
* HTTP/1.1..Hos
t: 239.255.255.2

KEY POINTS

Activity – Wireshark Demo



KEY POINTS



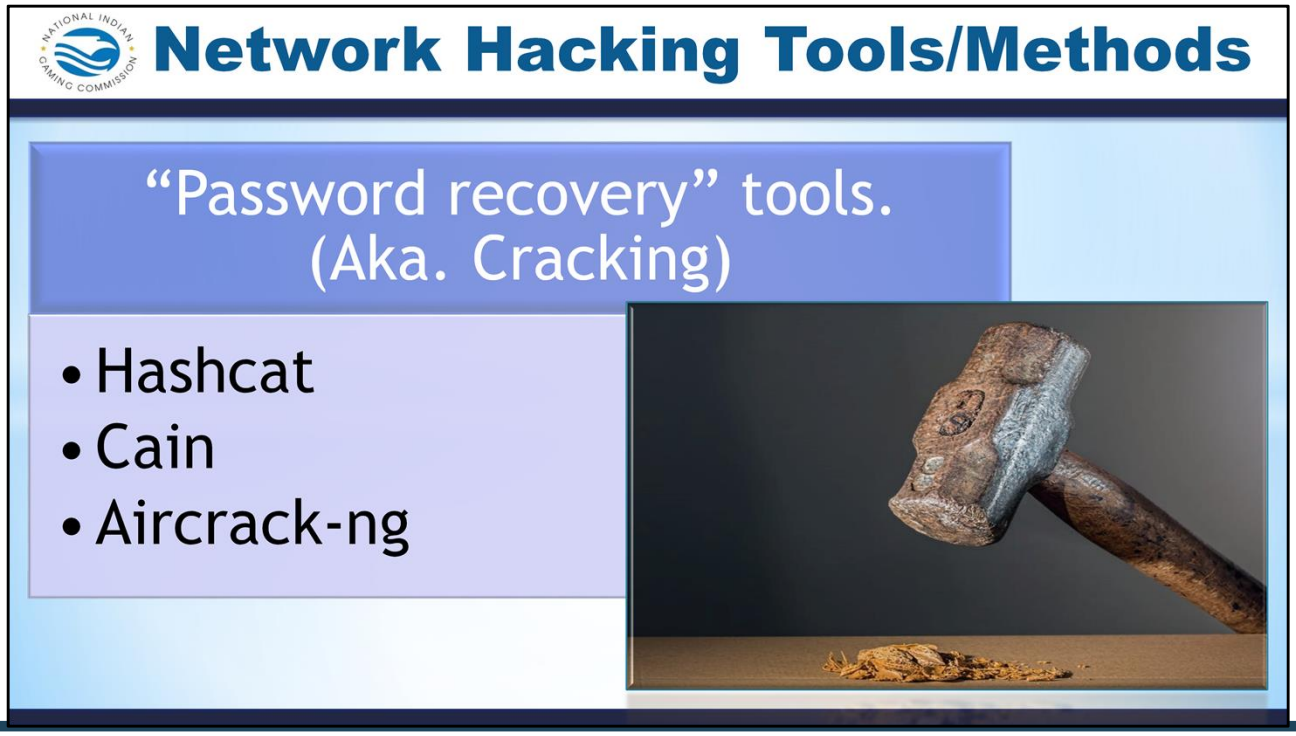
KEY POINTS

Use encrypted transmission methods whenever possible.

Packet Sniffing Defenses

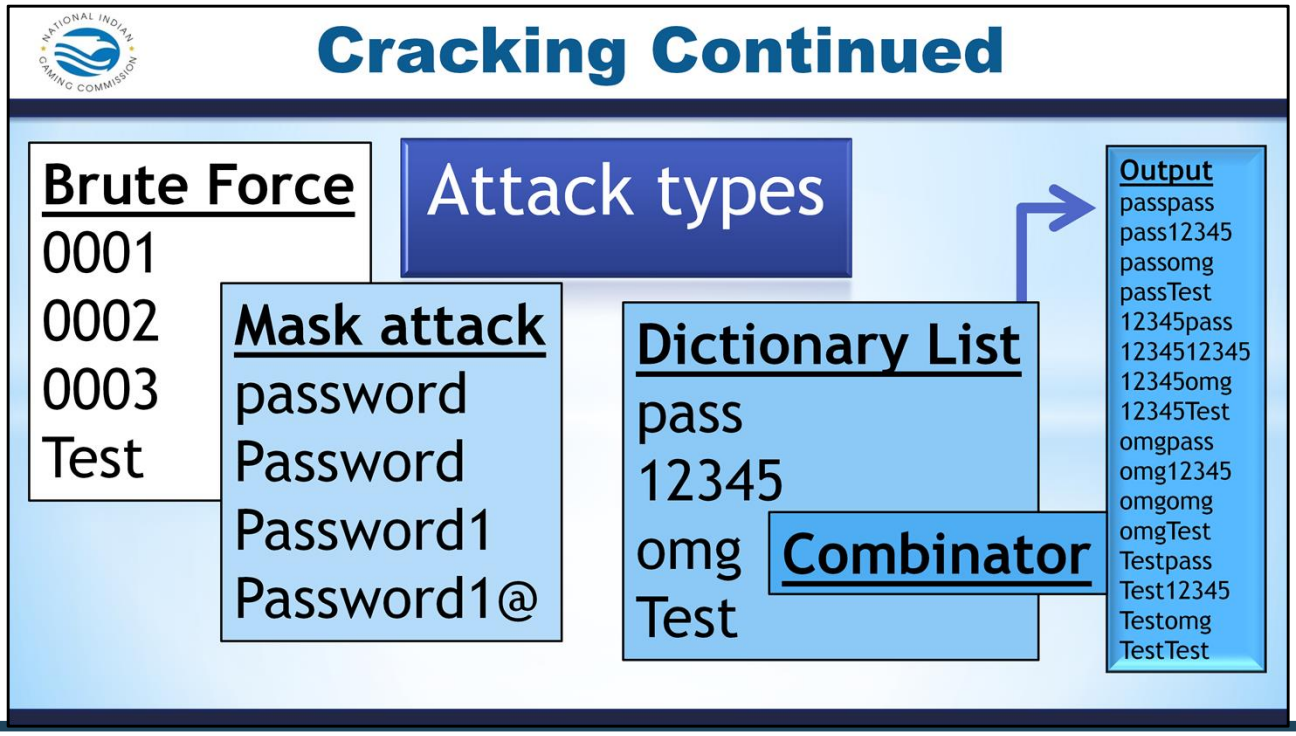
- **Restrict** physical access to the network.
- Use **encryption**.
- **Use MAC addresses.**
- Use **static IP address and static APR**
- **Turn off** network identification broadcasts (ESSIS / BSSID)
- Use **IPv6** instead of IPv4 protocol.
- Avoid **outdated** Access Point encryption methods such as **WEP** encryption!

KEY POINTS



KEY POINTS

A variety of cheap free and easy to use password cracking tools exist



KEY POINTS

Different password guessing strategies exist and can easily be combined

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.

KEY POINTS

Most encryption methods have ways of being decrypted therefore choose a strong method, a strong password, and change passwords often.

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

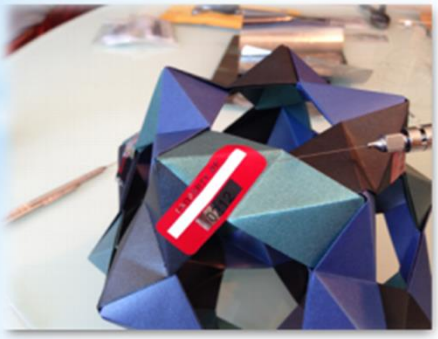
KEY POINTS

Sometimes vulnerabilities and data loss come from external or internal attackers, and sometimes from lack of education.

Human Error – Tamper Proof

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

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



KEY POINTS

Serialized, tamper evident seals are useful but only when paired with random file signature checks.
Simple techniques exist to hack both adhesive based and non-adhesive based seals.

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

KEY POINTS

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

CITIZENS BANK
Not your typical bank.®

Security key: qjkjaxaqwrq

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 update 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.

KEY POINTS
Phishing can be email based but also via phone.

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

KEY POINTS

Conformity – people naturally avoid confrontation
Diffusion of responsibility – It's not my problem. Not my job.
Friendliness – Name dropping, gathering info (your favorite team, your first car)

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

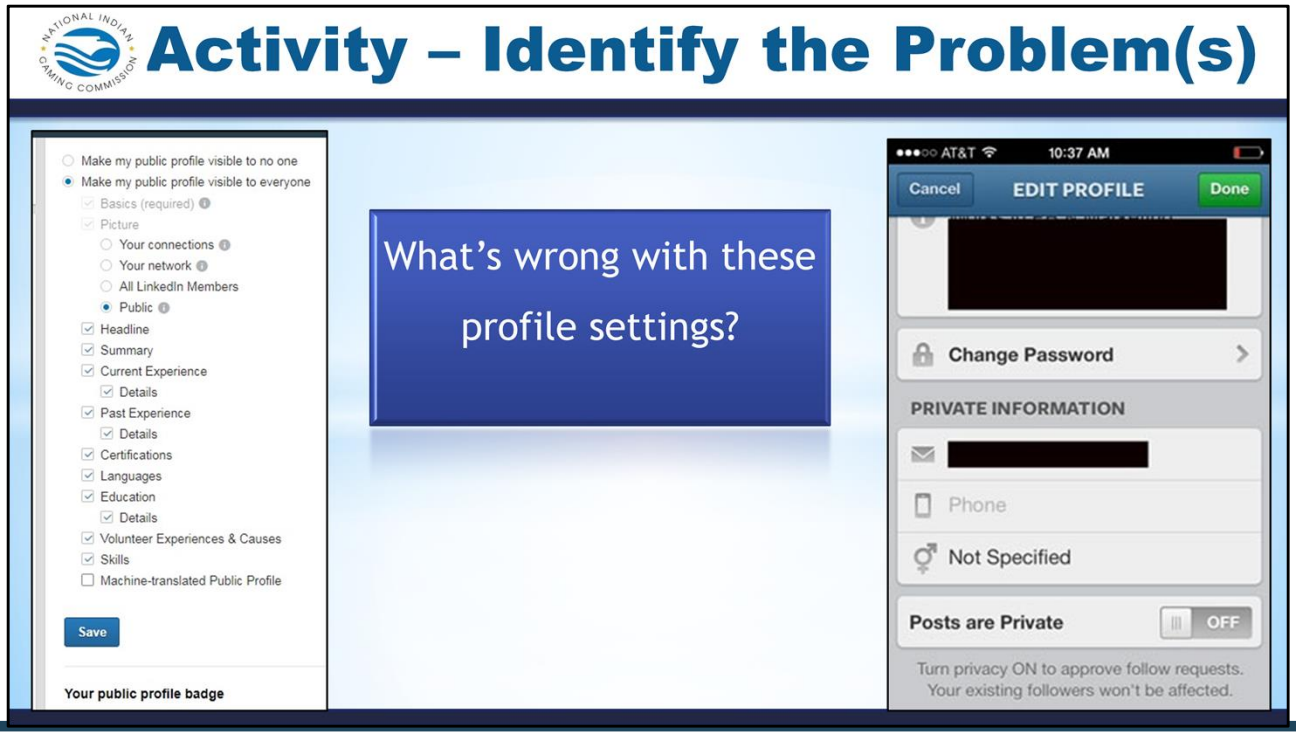
KEY POINTS

Human Error – Social Media

Tips for securing your online profile

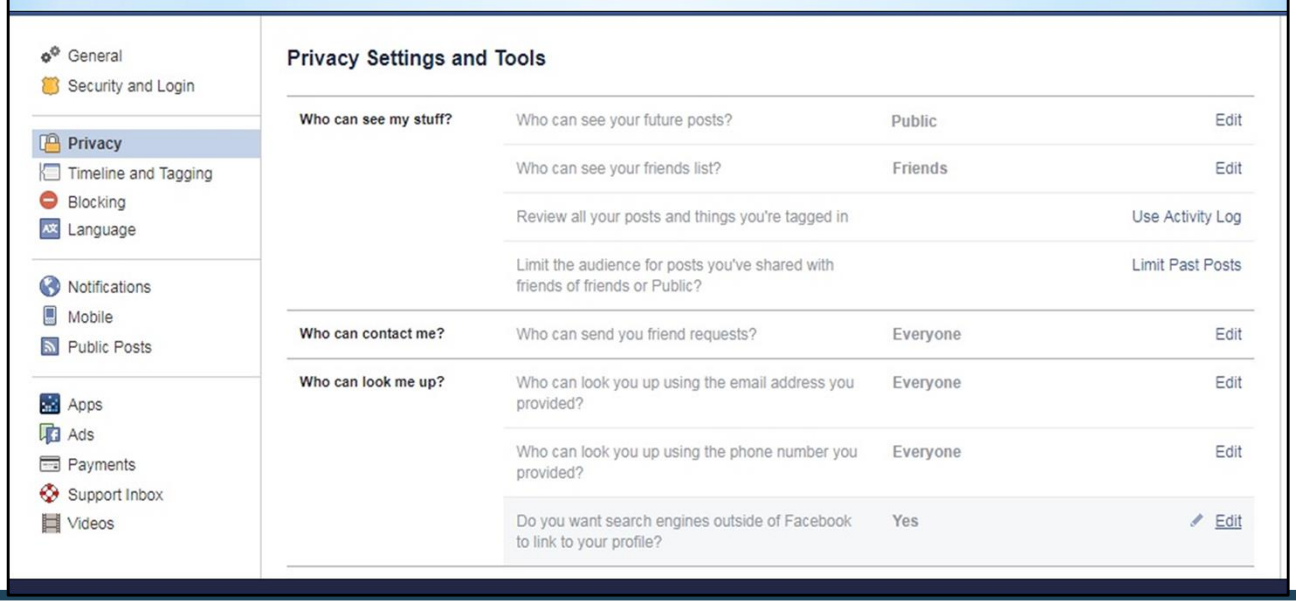
> Carefully choose your audience. (Friends, friends of friends, public)
> Use a Secret Email Address
> Secure Those Security Questions
> Set Up Login Notifications (dual factor auth)
> Don't link accounts

KEY POINTS

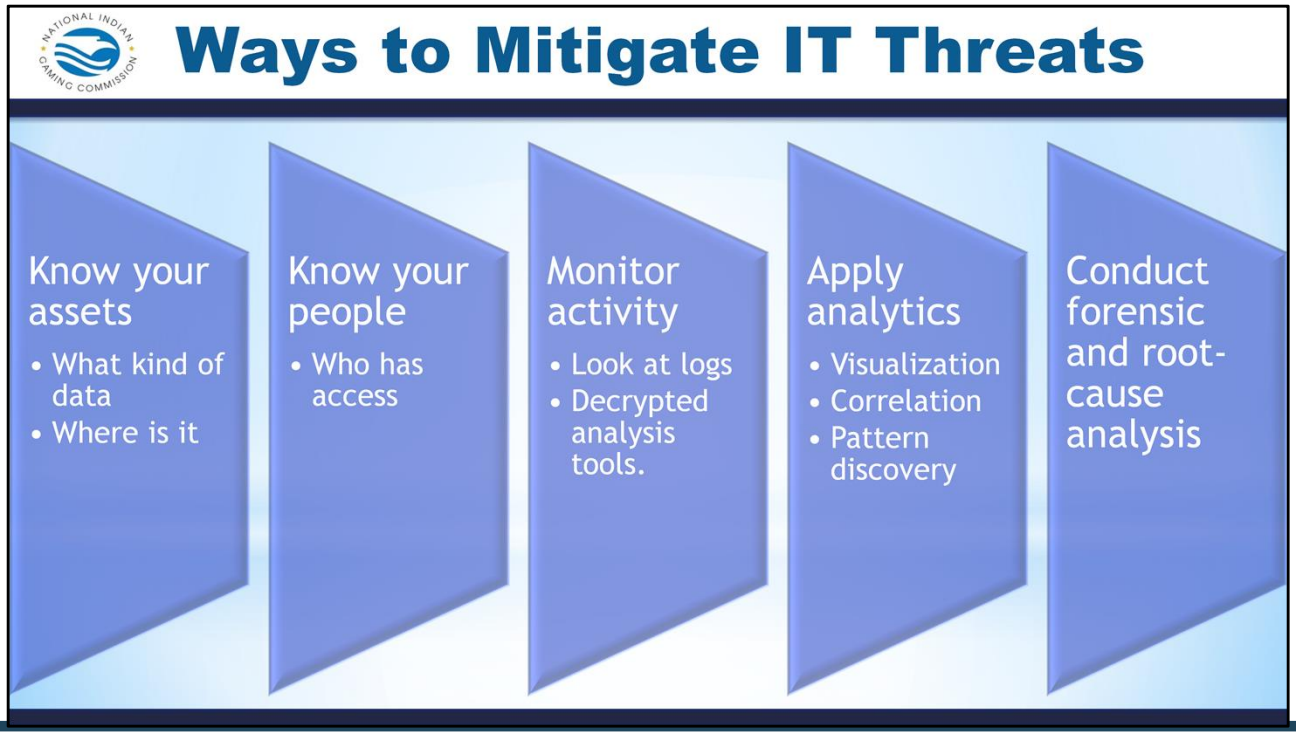

Activity – Identify the Problem(s)
Make my public profile visible to no one
Make my public profile visible to everyone
Basics (required)
Picture
Your connections
Your network
All LinkedIn Members
Public
Headline
Summary
Current Experience
Details
Past Experience
Details
Certifications
Languages
Education
Details
Volunteer Experiences & Causes
Skills
Machine-translated Public Profile
Save
Your public profile badge
What's wrong with these profile settings?
AT&T
10:37 AM
Cancel
EDIT PROFILE
Done
Change Password
PRIVATE INFORMATION
Phone
Not Specified
Posts are Private
OFF
Turn privacy ON to approve follow requests.
Your existing followers won't be affected.

KEY POINTS

Activity – Identify the Problem(s)



KEY POINTS


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

KEY POINTS

On the Horizon

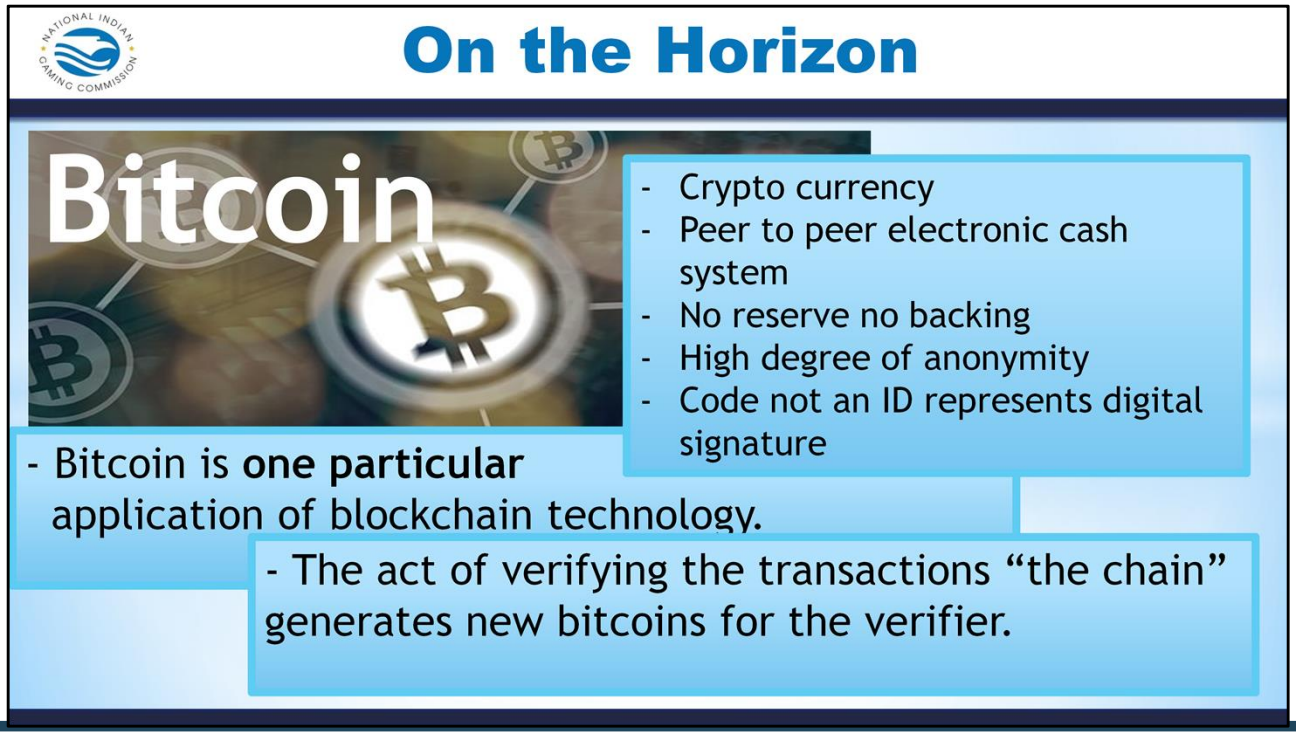
Blockchains, Bitcoin, Ether, and Crypto-currencies

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.

KEY POINTS

Blockchain technology is new and rapidly developing.
Blockchain is to Bitcoin, what the internet is to email.



KEY POINTS

- Relevant to casinos as the potential exists for money laundering.
- Illegal marketplaces.

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

KEY POINTS

Crypto coin technology will likely become more prevalent in other industries and scenarios.

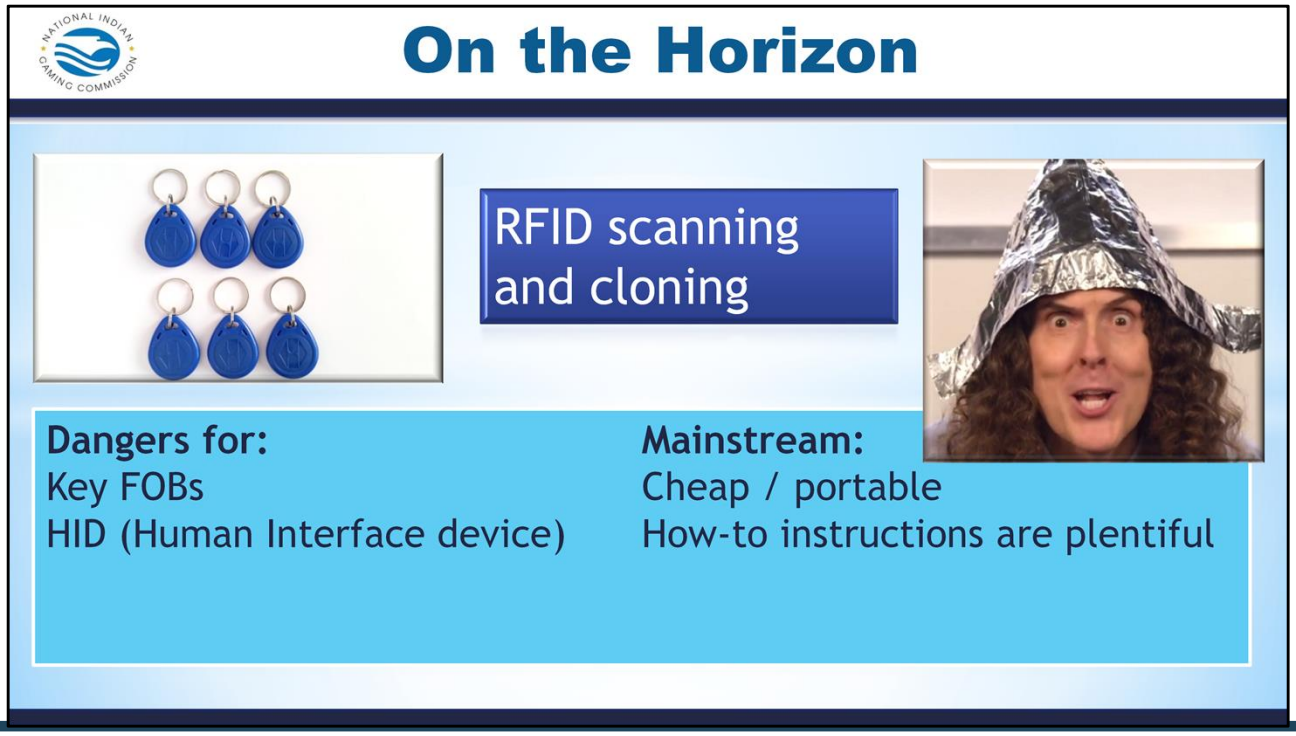
On the Horizon

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

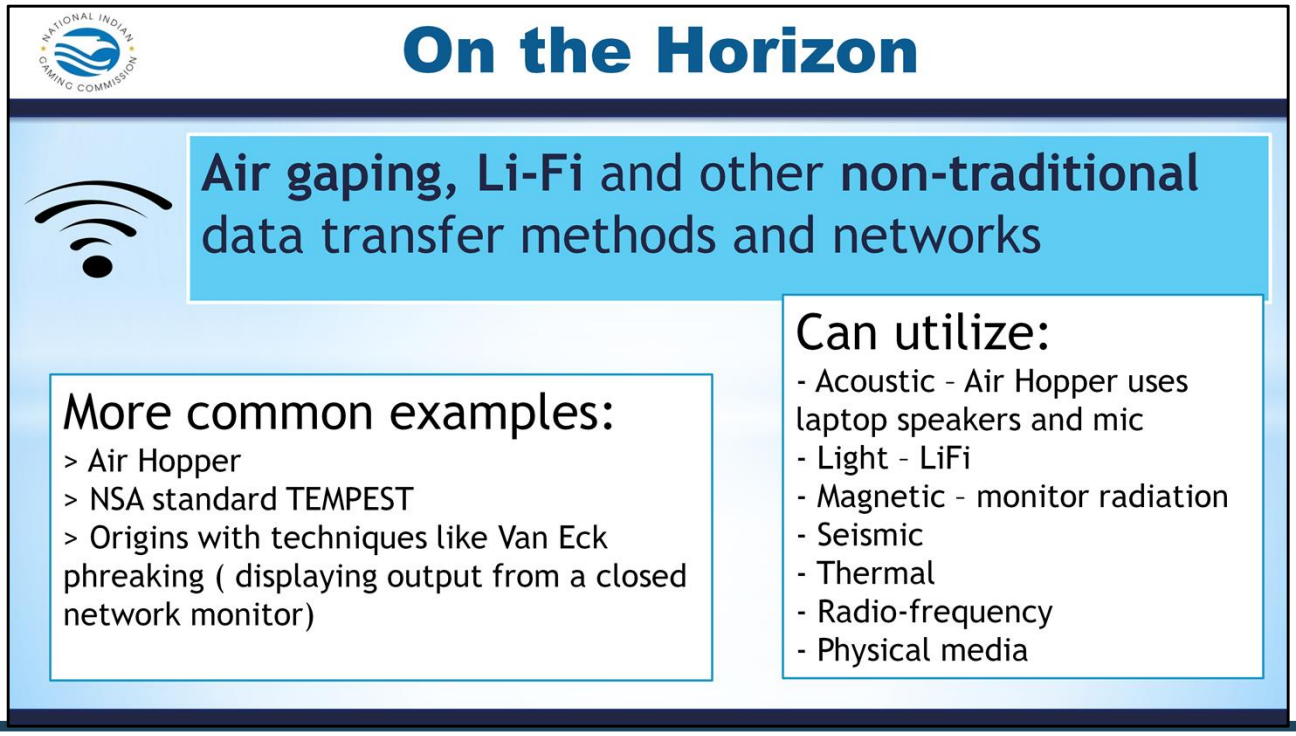
Source: http://www.bbc.com

KEY POINTS



KEY POINTS

Don’t rely on key management systems alone. Other controls are required.

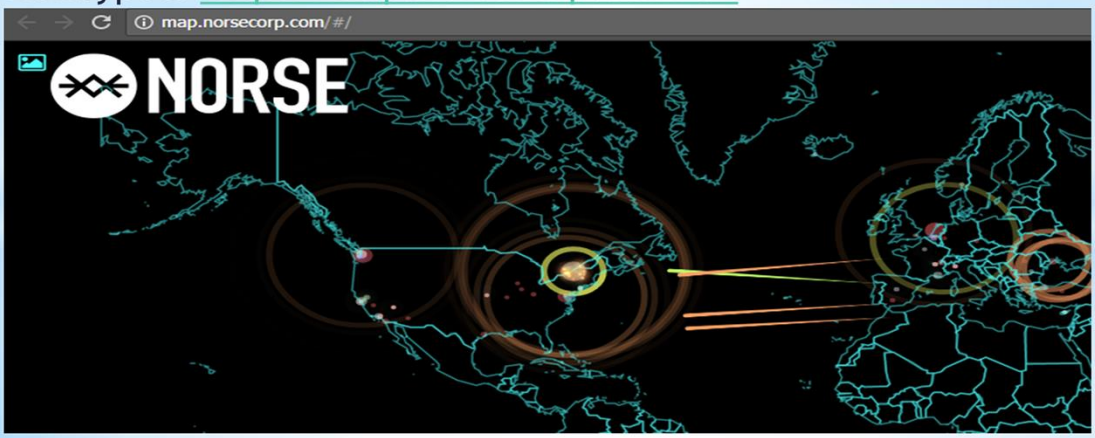


KEY POINTS

Technologies evolve, and not all data is sent via WiFi or other networks.

On the Horizon

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



KEY POINTS

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

KEY POINTS


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

KEY POINTS

KEY POINTS

Poll Title: Course Eval IT-108 IT Threats

https://www.polleverywhere.com/surveys/Em2QWMJXh