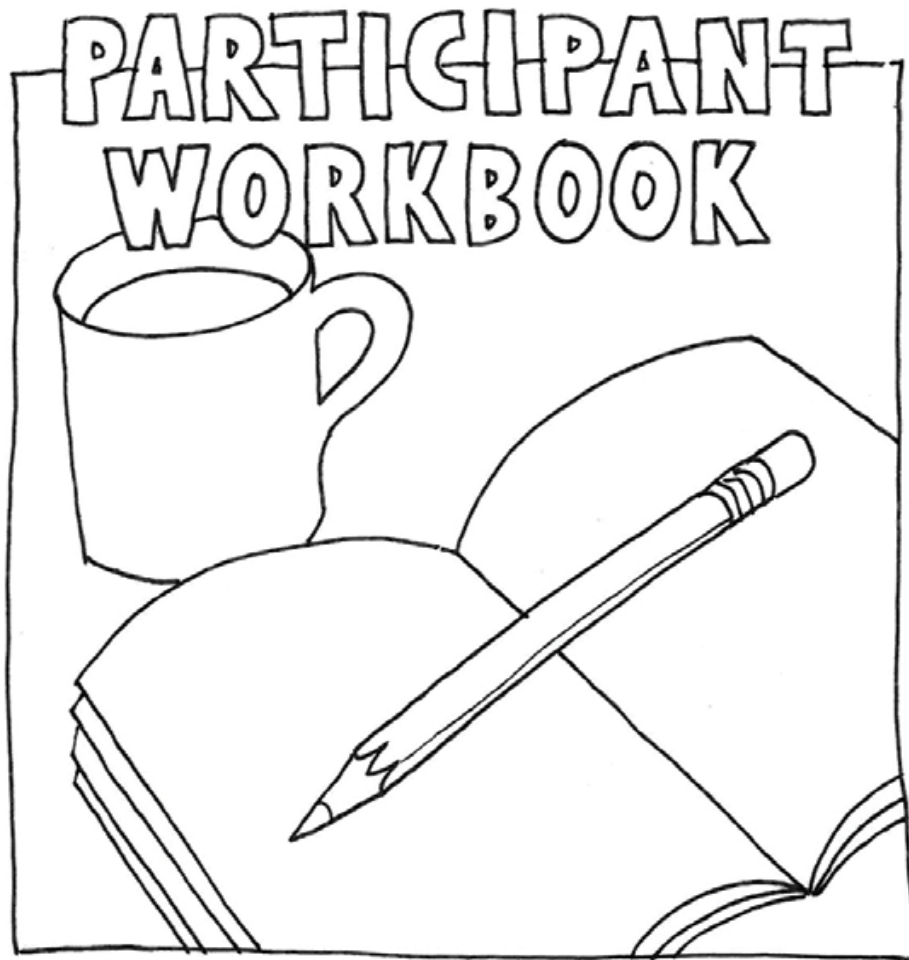




IT Boot Camp



Information Technology Threats



NOTES

[illegible]

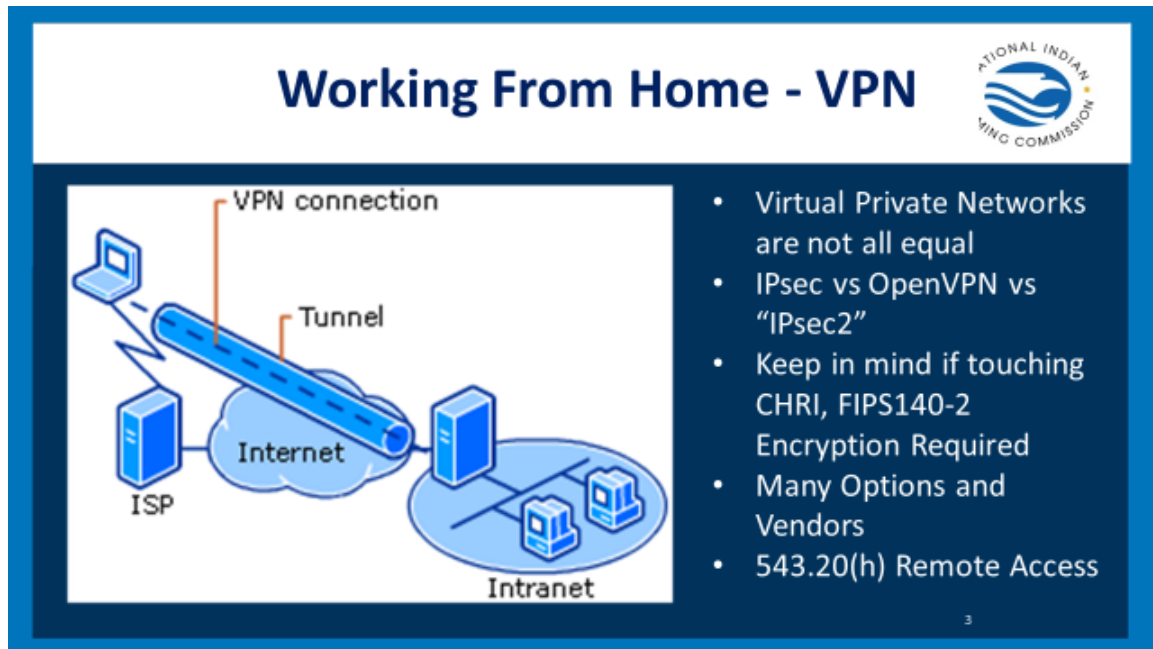
Training Overview



- Review New and Evolving Threats on the Horizon
- Explore Persistent and Trending Threats for 2021
- Define Threat Mitigation Techniques

NOTES

[illegible]

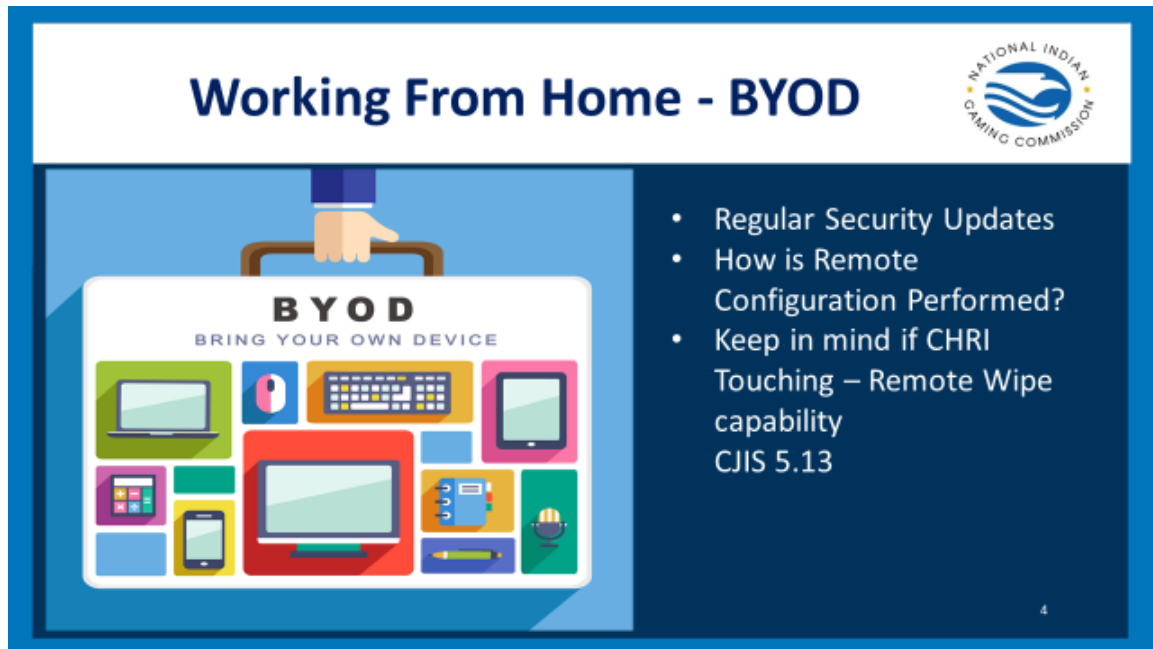


A VPN allows a secure tunnel through the internet to connect one computer or network to another computer or network.

OpenVPN can be the most secure if properly configured and regularly updated.

NOTES

[illegible]



How are devices configured remotely in a social distancing world? Many VPNs require a lot of manual configuration.

CJIS touching “mobile” devices need to have remote wipe capability.

NOTES

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

Working From Home - Conferencing



- How Secure Is It?
- What Configuration is Needed to Create or Join? (543.20(e) Logical Security)
- “Zoombombing”
- Where and what kind of Data is Stored? (CJIS 5.10)

5

With stay-at-home orders, there has been a massive and sudden increase in the usage and reliance on various video chat services.

As with any third party internet based system, we need to be aware of what kind of data is stored and where it is stored.

NOTES

[illegible]

Persistent Threat - Ransomware



A graphic illustrating a ransomware attack. It features a blue background with circuit-like patterns and several gold Bitcoin coins. Overlaid on this is a white rectangular box with a red border. Inside the box, there is a red and white shield icon on the left. To the right of the shield, the text reads: "RANSOMWARE ATTACK" in bold red letters, followed by "Your personal files are encrypted" in red, "You have 5 days to submit the payment!!!!" in smaller red text, "To retrieve the Private key you need to pay" in red, and "Your files will be lost" in small black text at the bottom.

- Malicious Software is Executed Remotely
- Critical Files are Encrypted
- Payment is Demanded to Decrypt Files
- Attackers can Wait Months to Strike.

6

Source: SOPHOS - “State of Ransomware 2020”

<https://secure2.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf>

NOTES

Persistent Threat - Ransomware



The illustration shows a laptop screen with the word 'Ransomware' at the top. On the screen is a yellow folder icon with a white padlock. A hand from the left, wearing a striped sleeve, holds a large white key over the padlock. Another hand from the right, wearing a black suit sleeve, holds a fan of green banknotes with dollar signs.

- Trending up in 2019 and 2020
- Backups More Effective than Paying
- Strategy Changing
- BEC (Business Email Compromise)
- Cryptocurrency Mining
- Cloud Backups Hit Too

Source:
SOPHOS – State of Ransomware 2020

7

94% of organizations whose data was encrypted got it back. More than twice as many got it back via backups (56%) than by paying the ransom (26%).

NOTES

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and extend across the width of the page. There are no margins, text, or other markings on the paper.





NIGC will sometimes release Tech Alerts with details about specific vulnerabilities

NOTES

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and extend across the width of the page. There are no margins, text, or other markings on the paper.

Why?

Why is Ransomware So Common?



- Phishing and Other Social Engineering Attacks
- Poor User Controls
- Poor Logical Security
- Insufficient Data Backups
- User Education

543.20(f)

543.20(e)

543.20(j)




Ransomware continues to be profitable for thieves and attackers in part, because of the prevalence, ease, and cost effectiveness of phishing and other types of social engineering attacks.


Damage is most strongly felt when there are insufficient data backups. The attacker cannot ransom something that has a copy elsewhere.

NOTE: _____

Persistent Threats – Social Engineering



SOCIAL? ENGINEERING



"Any act that influences a person to take an action that may or may not be in their best interest." – Social Engineer Inc.

"Social engineering is the act of tricking someone into divulging information or taking action, usually through technology." - NortonLifeLock

Many Types:

- Phishing
- Spear phishing
- Baiting
- Quid Pro Quo
- Vishing (Voice phishing)

11

NIGC uses industry standard software to automate much of the process of finding vulnerabilities.

Tenable Nessus and **Metasploit** are two of the most well known utilities.

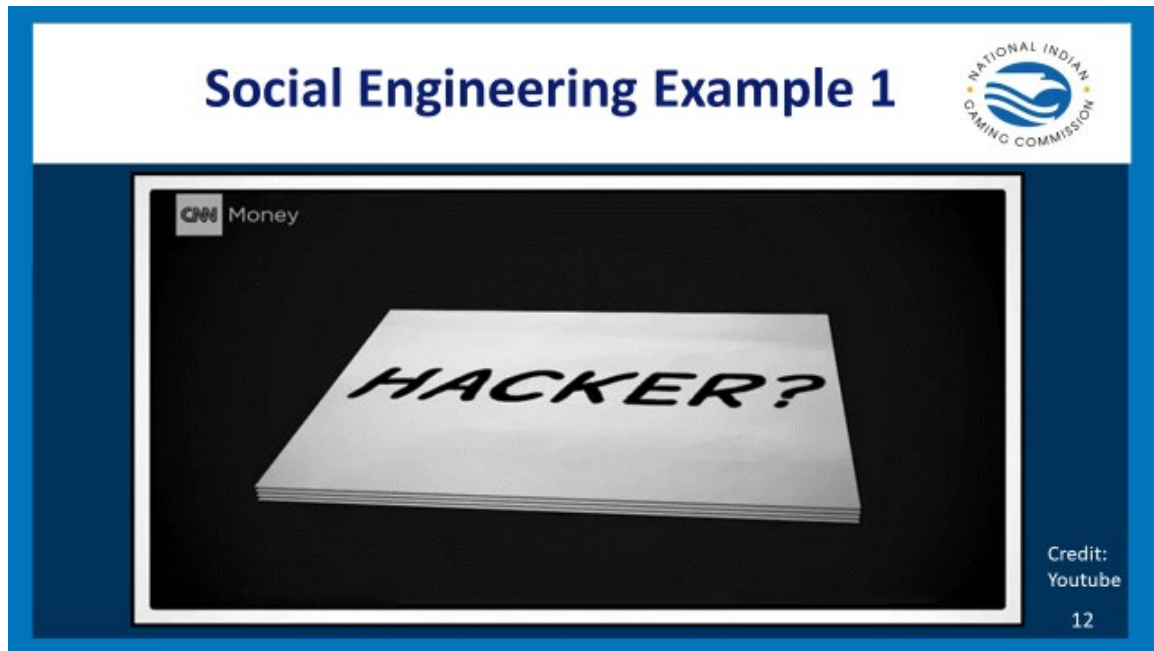
The respective software bases the severity of the vulnerabilities off published databases from:

- NIST (National Institute of Standards and Technology)
- CVSS (Common Vulnerability Scoring System)
- NVD (National Vulnerability Database)

See also:

<https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator?vector=AV:N/AC:L/Au:N/C:P/I:P/A:P>

NOTES



Video example of Social Engineering

Why is Social Engineering so dangerous?

- Because it can lead to any variety and manner of attacks.

NOTES

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

Social Engineering Targets/Tools



Many Types of Info. Targets

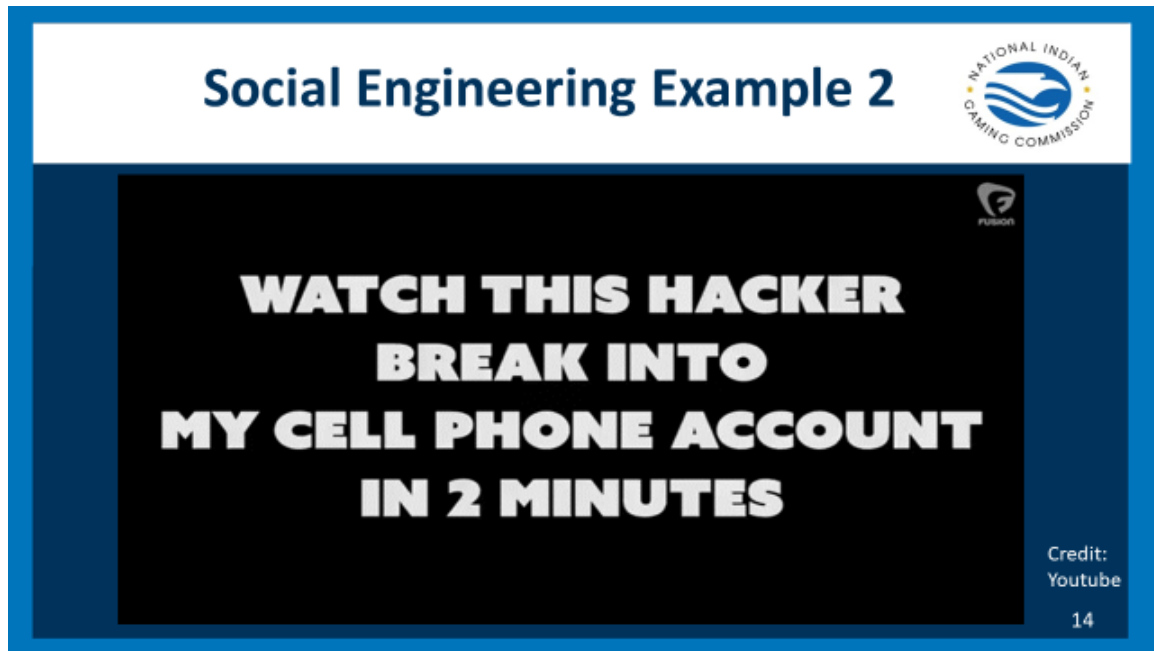
- Who Handles IT
- What Browser is Used
- What OS is in Use
- How Do they Open PDFs
- Who does Food Service, Janitor, Pest-Control, Trash Service
- Rem: Social Media, Job Sites, Hacker Sites.

13

Many types of information can be used by attackers to facilitate an attack.

NOTES

[illegible]



Hacking is not limited to just breaking into a computer.

Via Social Engineering, the process can be about:

- Influence
- Manipulation
- Elicitation
- Psychology
- Profiling
- Facial and Body Language
- Emotional hijacking
- Misdirection
- Information gathering

NOTES

For detailed steps and advice on formulating a Disaster Recovery Plan or Backup Continuity Plan see:
ITIL Continuity Management, also ISO 22301 and other industry standards.

Backup Continuity Plans



- ITIL Continuity Management
- ISO 22301
- Identify Critical Areas
- Identify Responsible Parties
- Identify Recovery Procedures
- Annual Testing - 543.20(j)(3)

15

Basic steps involve identifying critical areas, their respective responsible parties, and then documenting the recovery procedures.

Many of these policies and procedures may already be covered with 543.20(j)(3) in your annual testing of Data Backup procedures.

NOTES

Cybersecurity Insurance



- Read the Fine Print.
- Who is the Covered Party?
- What are the Covered Services?
- Who are the Approved Investigators?
- Exceptions? (ie. Act-of-War)


16

Strong Controls will minimize risks and level of damage of an attack, but some attacks are unavoidable, cyber insurance may be a viable risk reducing solution

- Make sure you read and understand the policy
- Know exactly which parties and services are covered
- Is there a specific third party investigator that must be utilized for payment to be approved?
- Watch out for exceptions such as act-of-war due to state sponsored actors. (i.e. Gov. vs. Gov.)


NOTES

Mitigating Risk



- Data Backups**
 - 543.20(j)
 - Recovery Procedures
 - Tested Procedures
- Incident Management**
 - 543.20(i)
 - BCP (Backup Continuity Plan)

17




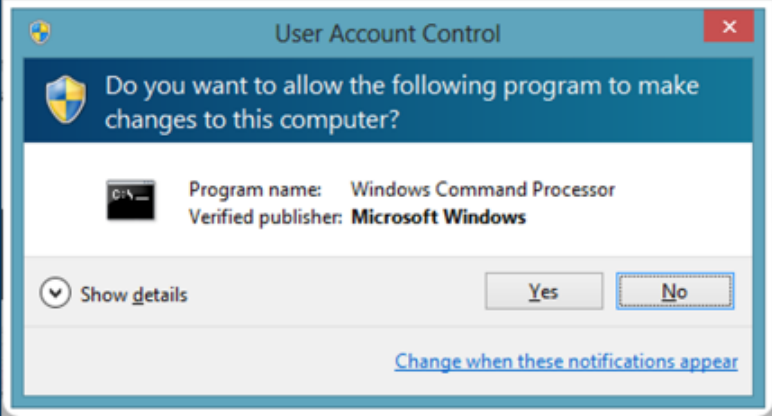
To reduce the impact after an attack has already occurred and damage has been done, it is important to have strong controls regarding data backups and incident management.

- Not just to have the controls, but to have documented the appropriate steps to take in the event of an attack.

NOTES

Mitigating Risks (Continued)





- Limit User Access
- Segregate Networks
- 543.20(f) User Controls

18


To reduce the scope of the damage of an attack beforehand and limit some of the harm an attacker could do.


User Access Controls can go a long way, by limiting what a hijacked system can see or do.

- Limit who has executable access
- Segregate networks to reduce damage and limit risk to other computers from compromised systems
- Remember 543.20(f)


NOTES

Mitigating Risks (Continued)





- Change Management
 - Patch Management
 - 543.20(g)
- User Education
 - Awareness Training
 - NIST SP 800-50



19

- Strong Change Management procedures are important.
-> Regularly check for and apply software/firmware updates and patches.
- User Education and awareness training can be one of the most effective ways to reduce risk.
-> NIST SP 800-50 outlines steps for creating a cybersecurity training program.
- <https://csrc.nist.gov/publications/detail/sp/800-50/final>

NOTES



Thank you for your participation and attending this session of the Information Technology Boot Camp!

After you log out you will receive a Survey. We ask that you complete the survey as the feedback helps us to get better at what we do!

We hope that you will join us for the next session.

NIGC Training can be reached at traininginfo@nigc.gov