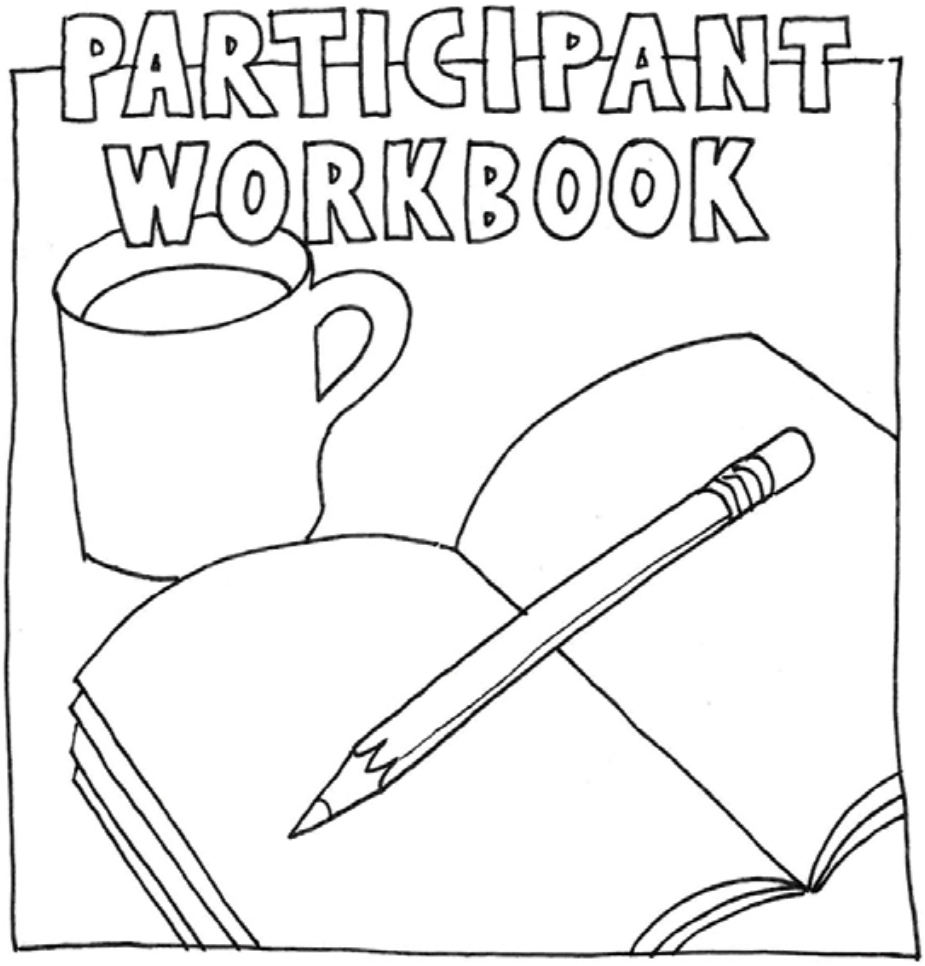
IT Boot Camp



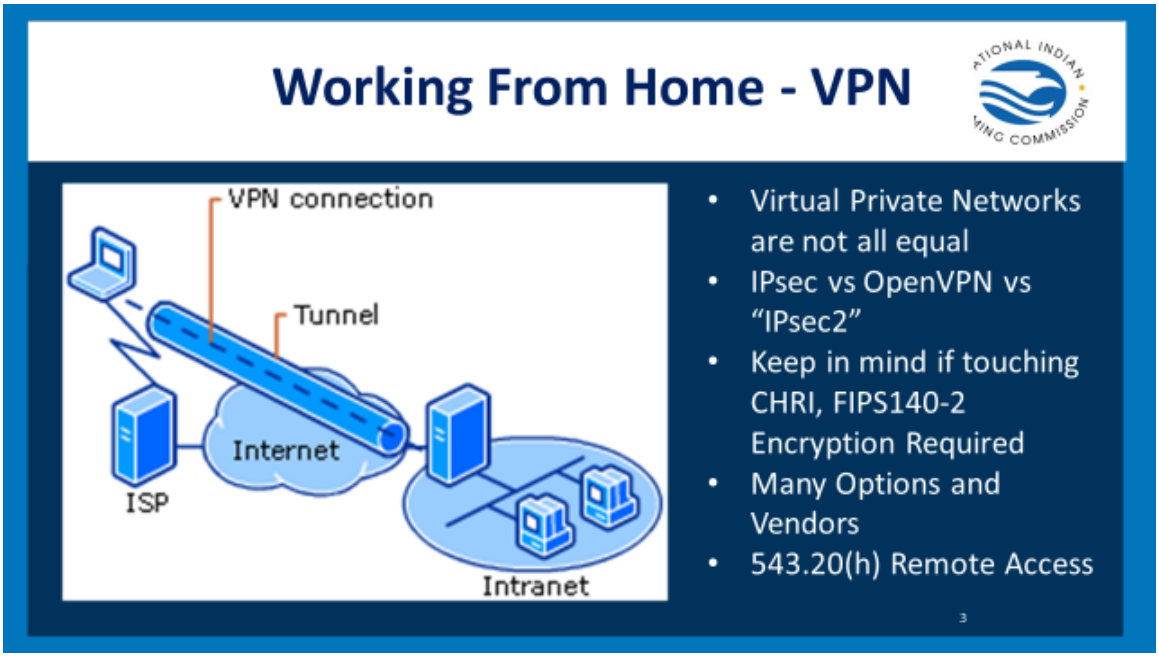
Information Technology Threats

Information Technology

NOTES


Training Overview
NATIONAL INDIAN GAMING COMMISSION
• Review New and Evolving Threats on the Horizon
• Explore Persistent and Trending Threats for 2021
• Define Threat Mitigation Techniques

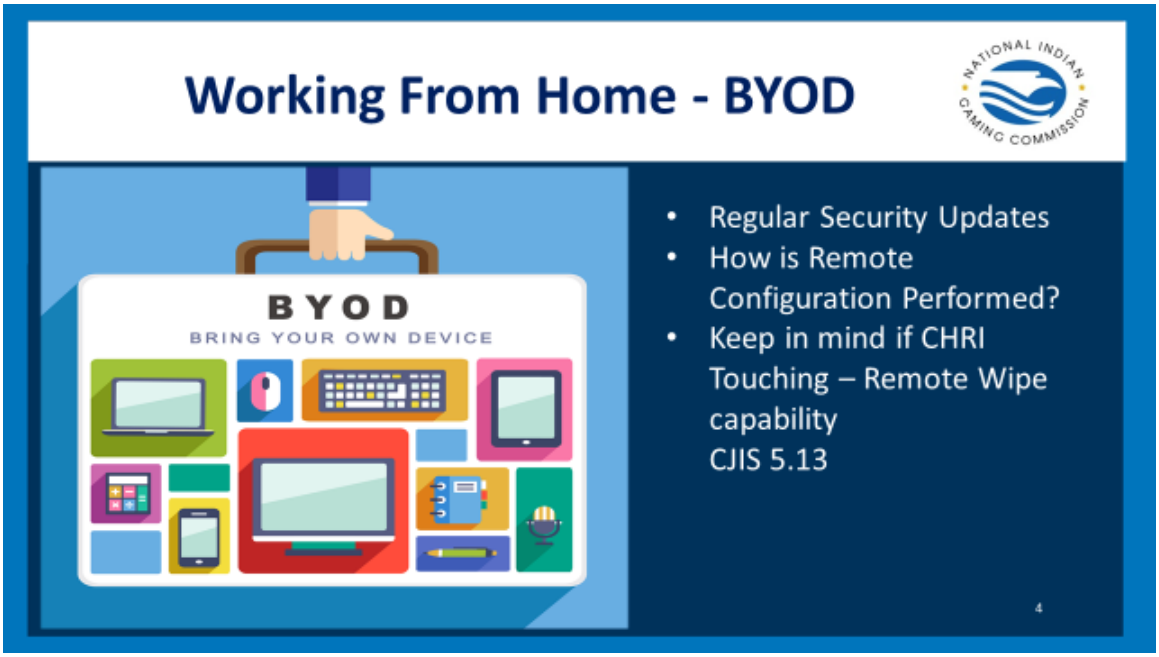
NOTES



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



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

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

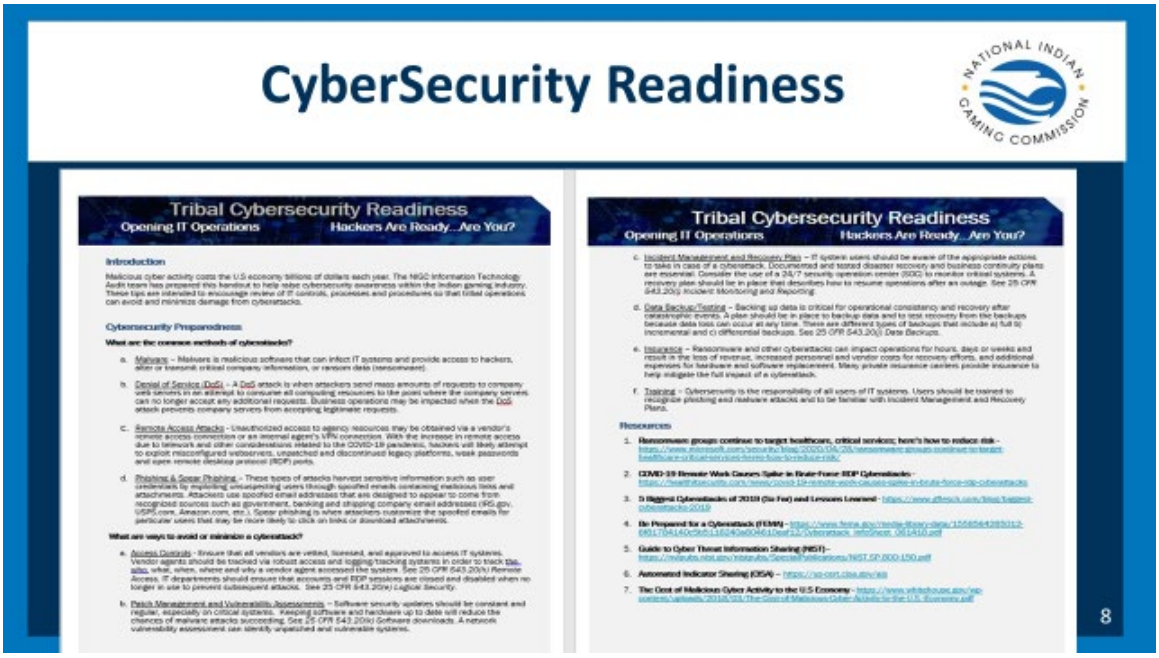
Source: SOPHOS - "State of Ransomware 2020"

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

NOTES

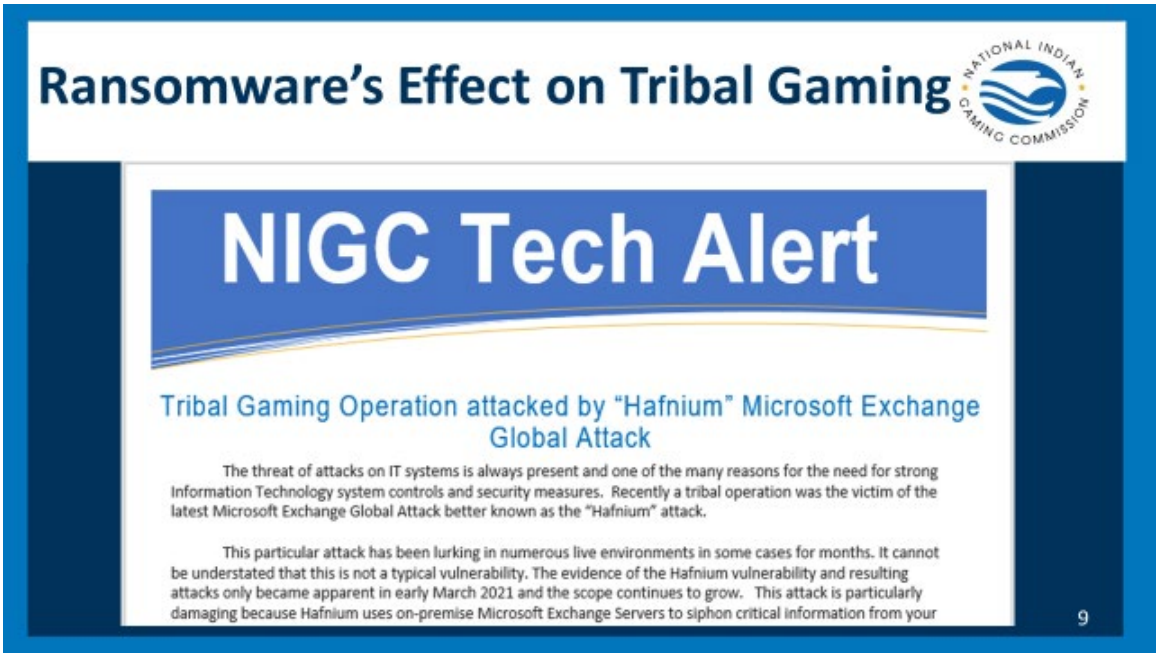
94% of organizations whose data was encrypted got it back. More than twice as many got it back via backups (56%) than by paying the ransom (26%).

NOTES



This document is available here:
https://www.nigc.gov/images/uploads/Tribal_Cybersecurity_Readiness.pdf

NOTES



NIGC will sometimes release Tech Alerts with details about specific vulnerabilities

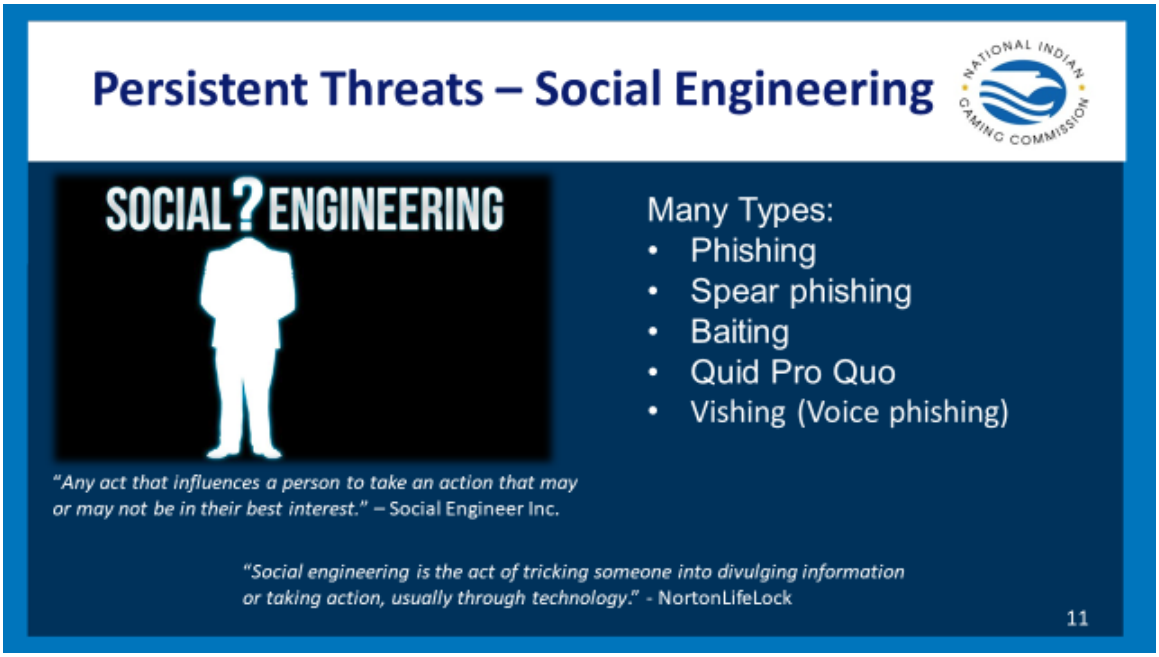
NOTES

Why?

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:



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

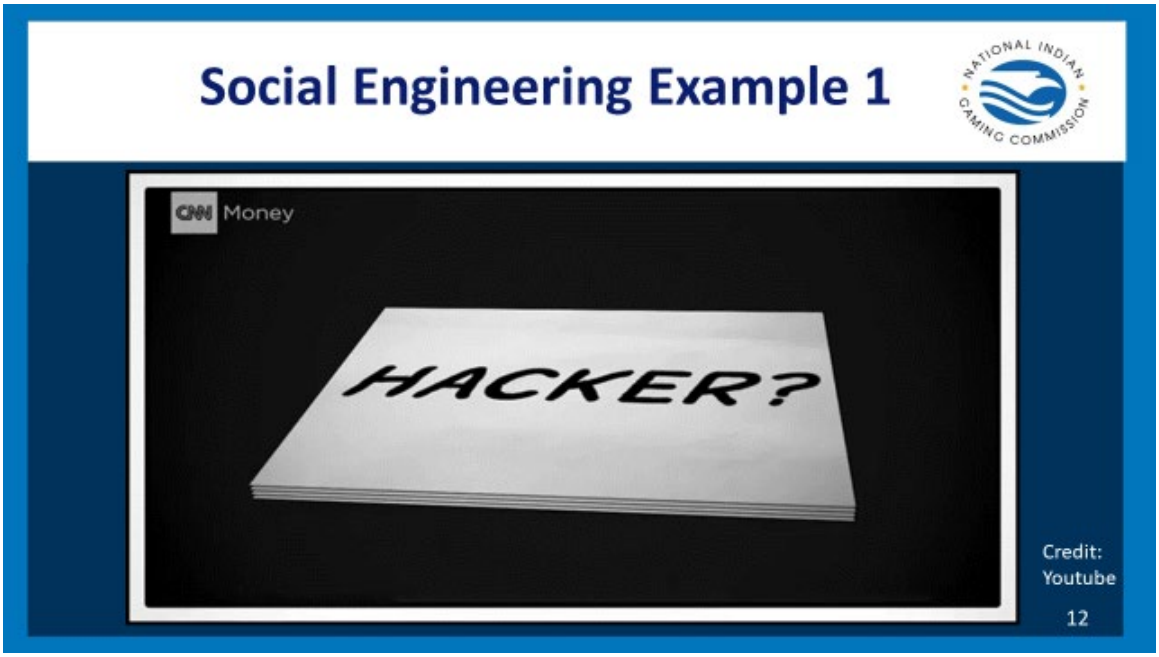
Tenable Nessus and **Metasploit** are two of the most well known utilities.

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

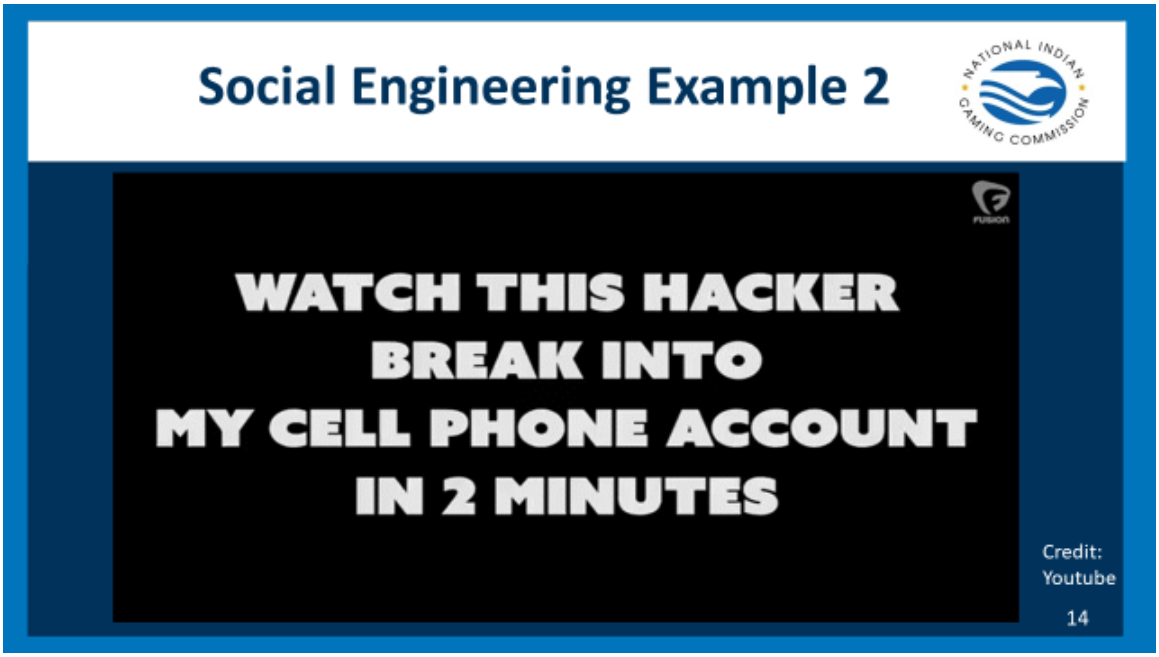
Why is Social Engineering so dangerous?

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

NOTES

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

NOTES



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.

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

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

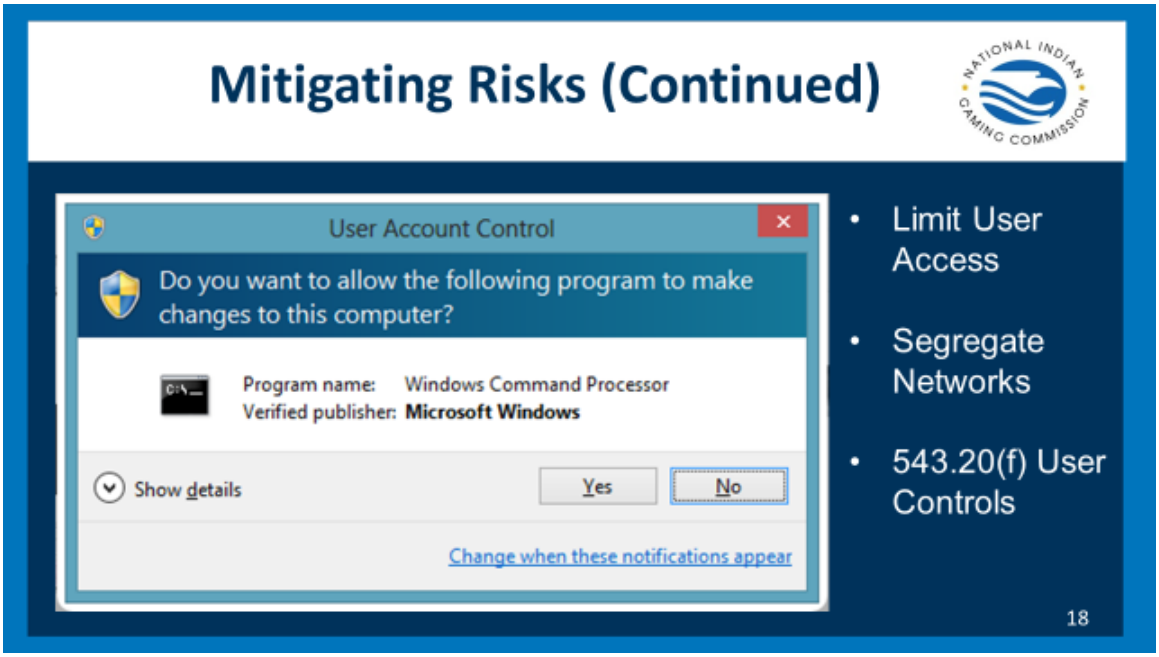
- Make sure you read and understand the policy
- Know exactly which parties and services are covered
- Is there a specific third party investigator that must be utilized for payment to be approved?
- Watch out for exceptions such as act-of-war due to state sponsored actors. (i.e. Gov. vs. Gov.)

NOTES

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

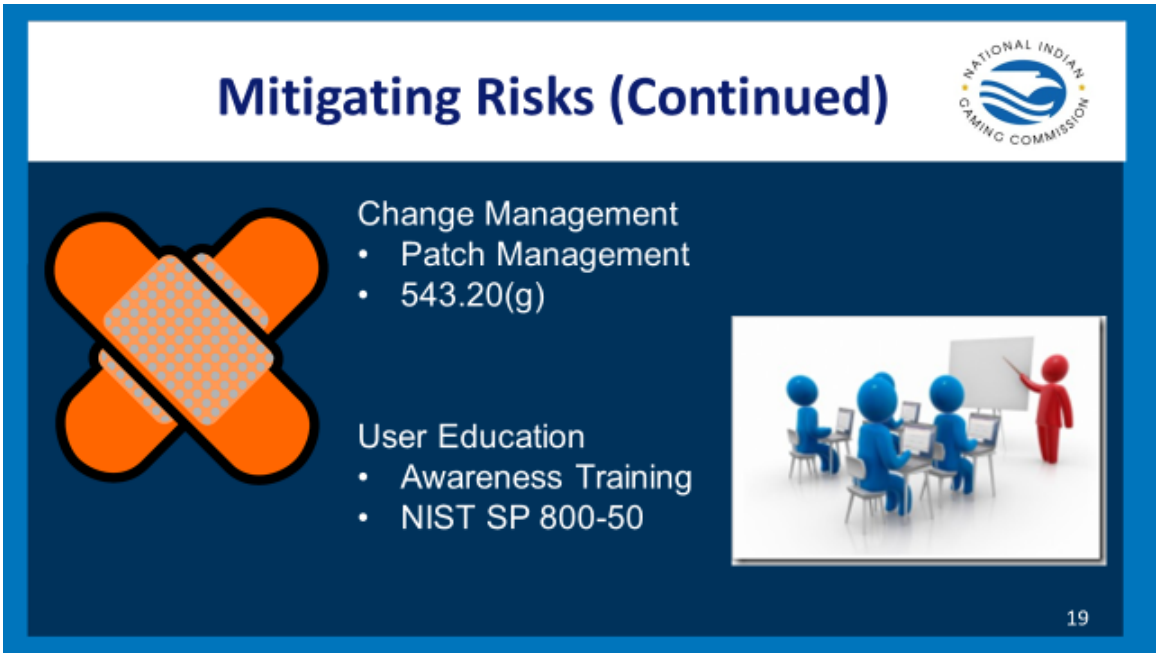


To reduce the scope of the damage of an attack beforehand and limit some of the harm an attacker could do.

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

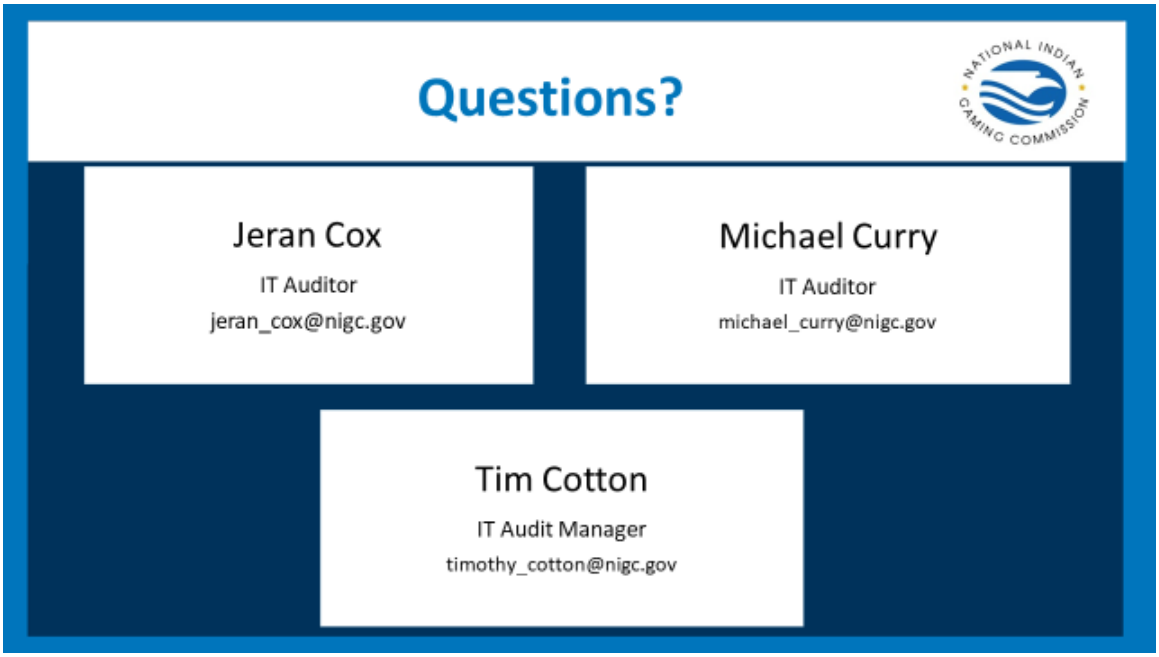
- Limit who has executable access
- Segregate networks to reduce damage and limit risk to other computers from compromised systems
- Remember 543.20(f)

NOTES



- 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