DigitalAcademy

Security awareness and tools to meet the challenges - OUTILNE

Description:

Security awareness and tools to meet the challenges

Introduction:

1. The historical roots of the challenge.

1.1.1. There is nothing new about information theft and manipulation. Only the tools and the risks have changed because of modern societal dependence on computers.

1.1.2. Computer security has become a modern issue because of our dependence on computing systems. The challenge hasn't changed – only the methods. The conflict is now one of security versus convenience.

1.1.3. How much risk you are willing to accept is a personal decision based on your own risk appetite. The goal of this presentation is to make you better aware of the risks to help you make that personal decision, and to present you with tools to minimize those risks.

2. The Cost:

2.1.1. Personal losses:

2.1.2. https://www.securityweek.com/cybercrime-losses-exceeded-10-billion-in-2022-fbi/#:~:text=The%20IC3's%202022%20Internet%20Crime,for%20%2427.6%20billion%20in%20losses.

3. How is information commonly compromised?

3.1.1. Impersonation
3.1.2. Interception
3.1.3. Substitution
3.1.4. Destruction
3.1.5. Misdirection (Social Engineering)
3.1.6. Commandeering
3.1.7. Implantation
3.1.8. Modification

4. Motives:

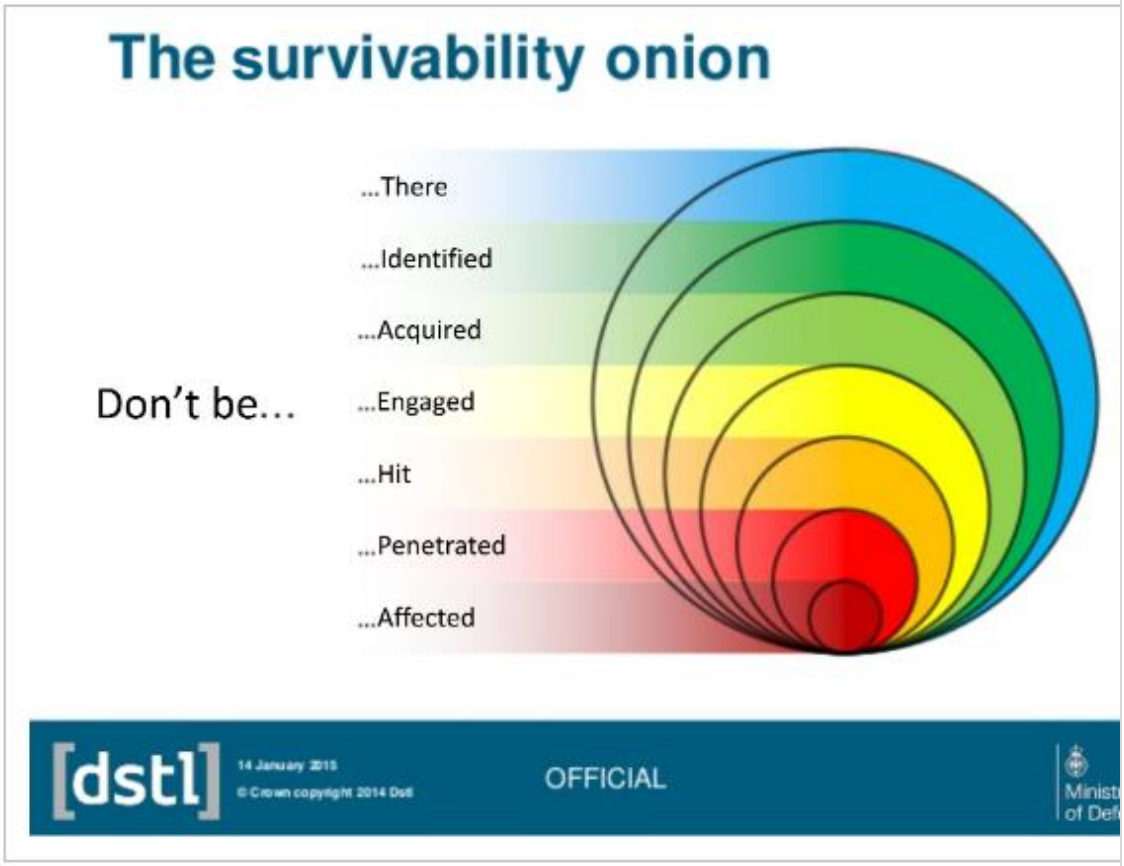
4.1.1. Theft/Fraud (MONEY!)
4.1.2. Experimentation
4.1.3. Extortion/Blackmail
4.1.4. Espionage

4.1.5. Humiliation

5. Actors:
- 5.1.1. Amateurs
- 5.1.2. Criminal Enterprises
- 5.1.3. Political Activists
- 5.1.4. Privateers
- 5.1.5. Nation-States
- 5.1.6. Competitors
- 5.1.7. Stunt Hackers and Unethical Cyber Security Actors

6. Countermeasures. Protecting yourself.CDs are
- 6.1.1. Skepticism: Don't believe everything you read!
  - 6.1.1.1.1. Text message exploits.
  - 6.1.1.1.2. Don't implicitly trust sites on the Web.
    - 6.1.1.1.2.1.1. How to use HTTPS
      - 6.1.1.1.2.1.1.1. Never trust a broken lock.
      - 6.1.1.1.2.1.1.2. HTTPS protocol basics. They trust you, but can you trust them?
      - 6.1.1.1.2.1.1.3. Don't submit anything to a HTTP site.
- 6.1.2. Physical access trumps everything (except good encryption).
  - 6.1.2.1.1. Don't let others use your systems.
  - 6.1.2.1.2. Physically secure unattended systems in untrusted environments.
    - 6.1.2.1.2.1.1. Is your car trustworthy?
      - 6.1.2.1.2.1.1.1. Always store your laptop when you leave – not when you arrive.
  - 6.1.2.1.3. USBs and CDs are physical access.
- 6.1.3. Passwords and other bad behaviors.
  - 6.1.3.1.1. Passwords are passe.
    - 6.1.3.1.1.1.1. Use two-factor or two-step authentication whenever possible.
    - 6.1.3.1.1.1.2. Passwords: the Good, the Bad, and the Ugly.
      - 6.1.3.1.1.1.2.1.1. The two enemies of reliability are coupling and complexity.
      - 6.1.3.1.1.1.2.1.2. Don't couple passwords between sites.
      - 6.1.3.1.1.1.2.1.3. Strategy for decoupling.
      - 6.1.3.1.1.1.2.1.4. Avoiding complexity.
      - 6.1.3.1.1.1.2.1.5. Modern password construction advice.
      - 6.1.3.1.1.1.2.1.6. Coping with ancient password policies.
      - 6.1.3.1.1.1.2.1.7. Why the old policies still exist?
      - 6.1.3.1.1.1.2.1.8. How to accommodate the legacies.
- 6.1.4. Pathogens, Parasites, and Malignancies:
  - 6.1.4.1.1. The same mechanisms that afflict humans also make computers "sick"
    - 6.1.4.1.1.1.1. Pathogens: Computer viruses.
    - 6.1.4.1.1.1.2. Parasites: Network propagating worms.
    - 6.1.4.1.1.1.3. Malignancies: Bad, naive, and poorly designed software.

6.1.5. Surviving the Cyber War:



6.1.6. https://zslpublications.onlinelibrary.wiley.com/doi/full/10.1111/jzo.12682

6.1.7. Don't be there:

6.1.7.1.1. Don't expose anything that isn't necessary.

6.1.7.1.2. Keep your personal information off the Web.

6.1.7.1.3. Assume whatever you post can be exploited by people with the worst possible motives.

6.1.7.1.4. Remember whatever you post is eternal.

6.1.7.1.5. Remove unnecessary software.

6.1.8. Don't be identified:

6.1.8.1.1. Use HTTPS that obscures the details of your communications.

6.1.8.1.2. Commercial VPNs are of limited benefit in hiding your identity,

6.1.9. Don't be acquired:

6.1.9.1.1. Protect your personal log in credentials.

6.1.9.1.2. Use two=factor/two-step authentication wherever possible.

6.1.9.1.3. Don't reuse passwords.

6.1.10. Don't be engaged.
- 6.1.10.1.1. Be aware of social engineering attacks.
  - 6.1.10.1.1.1.1. Spoofing
  - 6.1.10.1.1.1.2. Masquerading
  - 6.1.10.1.1.1.3. Misdirection

6.1.11. Don't be hit:
- 6.1.11.1.1. Install patches promptly
  - 6.1.11.1.1.1.1. When a patch/update is released – the countdown has started.
    - 6.1.11.1.1.1.1.1. Malicious parties will busily reverse engineer the patch.
- 6.1.11.1.2. Use and update anti-virus software (even if the protection is minimal)

6.1.12. Don't be penetrated
- 6.1.12.1.1. Install a firewall. Ideally, also set access controls on your edge device: router.
- 6.1.12.1.2. Don't place unknown or untrusted devices on your network.
- 6.1.12.1.3. Remember that USB drives are physical access.

6.1.13. Don't be affected:
- 6.1.13.1.1. A good backup is your last line of defense.
  - 6.1.13.1.1.1.1. Practice restoring your backups.
  - 6.1.13.1.1.1.2. Beware of network-based backup solutions.

6.1.14. Closing:
- 6.1.14.1.1. Review of high points.

Goals:

- ⇨ Increase Awareness: Raise awareness of the risks and challenges associated with information theft and manipulation in the digital age.
- ⇨ Understand the Cost: Highlight the financial impact of cybercrime and the losses incurred by individuals and organizations.
- ⇨ Identify Common Compromises: Explore common methods of compromising information, such as impersonation, interception, substitution, destruction, and social engineering.
- ⇨ Explore Motives: Examine the motives behind cyber-attacks, including theft/fraud, experimentation, extortion/blackmail, espionage, and humiliation.
- ⇨ Identify Actors: Understand the different types of actors involved in cyber-attacks, ranging from amateurs to nation-states, and their motivations and capabilities.
- ⇨ Implement Countermeasures: Provide practical tools and strategies to protect against cyber threats, including scepticism, physical access control, password security, dealing with viruses and worms, surviving cyber warfare, and implementing backups.
- ⇨ Review and Recap: Summarize and reinforce the key points covered in the course to ensure understanding and retention of the material.

DigitalAcademy

Recommended Experience and Knowledge:
⇒ Basic understanding of computer systems: Participants should have a fundamental understanding of how computer systems work, including hardware, software, and networks. ⇒ Familiarity with operating systems: Knowledge of common operating systems such as Windows, macOS, and Linux is beneficial. Participants should be comfortable navigating and administering these systems. ⇒ Continuous learning mindset: Cybersecurity is a rapidly evolving field, and participants should have a willingness to stay updated with the latest trends, technologies, and best practices. Engaging in continuous learning and professional development will enhance their effectiveness as systems administrators.

14.06.2023 – Security Awareness and Tools to Meet the Challenges	
Overview This session should equip you with the necessary tools to address the challenges in our digital world. By understanding the historical roots of information theft, the personal costs of cybercrime, and the methods of compromise, we can adopt countermeasures such as scepticism, strong passwords, and regular patching to protect ourselves. Prioritizing physical security, minimizing exposure of personal information, and staying vigilant against social engineering are essential. Let's carry this knowledge forward and face the future confidently, safeguarding our digital lives.	
Time	Agenda Items
10:00 – 10:15	What the risks are?
10:15 – 10:20	Q&A
10:20 – 10:45	Who the attackers are?
10:45 – 11: 00	Questions and answers. Break
11:00 – 11:30	How to protect yourself
11:30 – 11:45	Q&A

DigitalAcademy

Course Lecturer Biography:

Patrick Bryant, M.Sc., CISSP, ISSAP, ISSMP, CISA

Patrick Bryant has been a Certified Information Systems Security Professional (CISSP) and Certified Information Systems Auditor (CISA) for twenty years. Patrick worked as a Cyber Security Subject Matter Expert at the Montenegro Ministry of Defense from 2020 to 2022 under a U.S. Department of Defense contract. He joined eGA as a consultant at the Ministry of Public Administration in 2023. Prior to his work in Montenegro, he was a Senior Information Security Advisor at NASA Ames Research Center where he was lead researcher of the Security Innovation Lab, as well as a countermeasures architect and incident responder. He also worked as a Licensed Private Investigator in California specializing in cyber-crime investigations where he was engaged by The Boeing Company, ExxonMobil, and Wells Fargo Bank as well as many other Silicon Valley enterprises. Patrick has extensive experience in incident detection and response, countermeasures development, technical risk minimization and security process development.