

IOSS New Face of Threats.

On Screen Text.

Course Welcome/Introduction.

Voice Over Script. Screen 1.

Welcome to the New Face of Threats training, presented by the Interagency OPSEC Support Staff and intended for OPSEC Practitioners.

The current technological landscape is vast; advancements seem to happen within the blink of an eye. This expansive cyber terrain has cultivated a dangerous cyber threat. The adversary's symbiotic relationship with technology allows them to exploit it for their own gains.

To stay ahead of the threat and remain secure, OPSEC practitioners must prepare. This requires a solid understanding of the vulnerabilities hidden within new technology, knowledge of the possibilities for exploitation inherent in the cyber world, and access to the best countermeasures available.

On Screen Text. Screen 2.

Course Objectives:

- Discuss cyber adversaries' intent and capabilities.
- Discuss wireless and mobile devices and applications targeted for critical information.
- Discuss computer vulnerabilities.
- Discuss emerging technologies and associated vulnerabilities.

Voice Over Script. Screen 2.

This course is intended to provide practitioners with the information needed to maintain Operations Security in the face of the Cyber Threat.

To do this, we'll explore several common cyber adversaries, their intent, and their capabilities.

For the purposes of this training, threat is defined as "An adversary with the intent and capability to target, collect, analyze, and employ intelligence to act against friendly assets or activities."

We'll also examine the vulnerabilities associated with wireless devices, portable devices, and Bluetooth technologies – and we'll address the countermeasures available for each piece of technology.

In addition, we'll discuss vulnerabilities resulting from mobile device data leakages, along with their associated countermeasures.

Finally, we'll take a look at emerging technologies, their associated vulnerabilities, and the potential countermeasures available.

Module 1.

On Screen Text. Screen 3.

Module 1: Cyber Adversaries.

Voice Over Script. Screen 3.

In this module, we'll discuss the types of cyber adversaries faced by today's OPSEC practitioner, their intent and capabilities, and the risks they ultimately pose to cyber security.

Adversaries listed in any of these general categories may use hacking as a tool, but an adversary's Internet usage does NOT have to include hacking.

On Screen Text. Screen 4.

Nation States.

Political organization in which a group of people who share the same history, traditions, or language live in a particular area under one government.

On Screen Text. Screen 5.

Nation States Intent.

Peacetime: Collect intelligence for economic, political, or military gain.

Wartime or Times of Crisis: Attack mission-critical infrastructure systems.

On Screen Text. Screen 6.

Nation States Capabilities – Information Warriors.

Cyber: Moderate to extremely skilled.

Risk: Accept high risk in pursuit of information operations.

Voice Over Script. Screen 6.

Nation States employ information warriors with a range of cyber skills, from novice to expert.

Foreign Intelligence Services generally provide full-time support to information collection operations conducted by Nation States. These activities may include the manipulation, degradation, or destruction of data and/or infrastructure within a targeted network.

Once at war, these information warriors are willing to take extraordinary risks in pursuit of their goals.

On Screen Text. Screen 7.

Nation States Capabilities – Foreign Intelligence Services.

Cyber: Sophisticated HUMINT, SIGINT, and OSINT.

Risk: Most are generally risk-averse; however, they are not above taking a physical risk such as breaking and entering to put a keylogger on a computer.

Voice Over Script. Screen 7.

Foreign Intelligence Services typically have access to sophisticated resources and advanced forms of Human Intelligence, Signals Intelligence, and Open-Source Intelligence.

Most Foreign Intelligence Services are risk-averse, but some are not above breaking and entering in order to steal information or plant listening devices.

Nations with progressive technology industry often have access to the cutting-edge tools needed to conduct life-cycle attacks.

Foreign Intelligence Services may rely on publicly available tools as well, concealing their own advanced capabilities in order to remain under the radar.

On Screen Text. Screen 8.

Organized Crime.

National and international crime syndicates, drug cartels, and well-organized gangs.

On Screen Text. Screen 9.

Organized Crime Intent.

Obtain huge profits through identity theft, extortion, corruption, and fraud.

On Screen Text. Screen 10.

Organized Crime Capabilities.

Cyber: Moderate to extremely skilled.

Risk: Senior members are risk-averse, low level members are risk-takers.

Voice Over Script. Screen 10.

Organized crime groups range from small-time, small budget groups to large, well-funded organizations.

While some of these groups may have in-house hackers, the majority is more likely to recruit individuals with hacking expertise.

The ultimate success of an organized crime group depends on its ability to avoid detection and apprehension by law enforcement. To that end, senior members remain risk-averse and instead use expendable, low-level foot soldiers to take major risks in pursuit of their goals.

Knowledge Check. Select the best answer.

Criminal enterprises participate in cyber crime in order to:

- a. Gain profits through identity theft, extortion, corruption, and fraud.
- b. Influence public opinion.
- c. Seek notoriety, adventure, or revenge.
- d. Cause citizens to question the government's ability to protect them.

The correct answer is "Gain profits through identity theft, extortion, corruption, and fraud." Criminal enterprises gain profits through the use of identity theft, extortion, corruption, and fraud as part of their cyber crime activities.

On Screen Text. Screen 11.

Terrorists.

Individuals who systematically use, or threaten to use violence to create a general climate of fear in a population, with the intent of furthering their goals, which are usually political.

On Screen Text. Screen 12.

Terrorists Intent.

Influence, shape, or change public opinion and recruit new members through cyber activities.

Cause uncertainty, insecurity, fear, and apprehension regarding the United States' ability to operate, protect, and deliver essential public services.

On Screen Text. Screen 13.

Terrorists Capabilities.

Cyber: Script kiddie to extremely skilled.

Risk: Willing to die for their cause.

Voice Over Script. Screen 13.

Terrorists possess cyber skill levels that range from "script kiddie" – the low-level hackers who rely on code written by others – to extremely proficient.

Terrorist groups range in size from a few isolated and uncontrolled individuals to much larger organizations with military structure and training. In some cases, Nation States may sponsor terrorist groups and provide them with the training, equipment, and political asylum they need to further their cause.

In all cases, terrorists are willing to take extreme risks and will die for their cause.

On Screen Text. Screen 14.

Economic Competitors.

Includes rival companies and foreign governments that use national assets to foster their internal industries.

On Screen Text. Screen 15.

Economic Competitors Intent.

Gain an economic competitive edge in the market.

On Screen Text. Screen 16.

Economic Competitors Capabilities.

Cyber: Moderate to extremely skilled.

Risk: Low risk tolerance for detection and attribution.

Voice Over Script. Screen 16.

Economic Competitors believe it's much more cost effective to steal technology than develop it themselves. To that end, these companies often employ fairly sophisticated HUMINT methods and may even resort to breaking and entering to steal information and/or technology.

Additionally, Economic Competitors with Nation State sponsorship may have a significant resource advantage over their rivals. Their cyber skill level typically ranges from moderately to extremely skilled. In general, Economic Competitors have a low risk tolerance for detection and attribution of their operations.

Knowledge Check. Select the best answer.

Economic competitors engage in cyber crime as a means to gain an advantage without investing the time, money, and skill in developing technology.

- a. True.
- b. False.

The correct answer is “True.” While it may seem sneaky and underhanded, some economic competitors find that **stealing** technology is more economically advantageous than **developing** technology.

Knowledge Check. Select the best answer.

Which cyber adversary is likely willing to die for their cause?

- a. Nation States.
- b. Organized Crime.
- c. Economic Competitors.
- d. Terrorists.

The correct answer is “Terrorists.” Terrorists are not only willing to die for their cause, but they’re willing to encourage others to die for it, too.

On Screen Text. Screen 17.

Hackers.

Individuals who gain unauthorized access to a computer system.

Includes recreational hackers, criminal hackers, and hacktivists.

On Screen Text. Screen 18.

Hackers Intent.

Recreational Hackers: Seek notoriety, adventure, revenge, and/or theft of services (theft of bandwidth, computing power, or storage in support of online activities).

Hacktivists: Seek to further a political or social cause.

On Screen Text. Screen 19.

Hacker Capabilities.

Cyber: Script kiddies to extremely skilled.

Risk: Low risk tolerance for attribution.

Voice Over Script. Screen 19.

Hackers possess skill levels that range from script kiddie to extremely proficient. They are masters of network attacks, which have a relatively low cost of entry. Both Recreational Hackers and Hacktivists use tools such as social engineering and OSINT to further their intent.

Despite their desire for notoriety, Hackers have a low risk tolerance for attribution. They are also unlikely to engage in physical attacks, preferring the anonymity provided by cyberspace.

Knowledge Check. Select the best answer.

Unskilled hackers who rely upon code written by others to attack computers and networks are called:

- a. Hacktivist.
- b. Super script.
- c. Black hatter.
- d. Script kiddie.

The correct answer is "script kiddie." Script kiddies rely upon code written by others to attack computer and networks. While they may lack coding skills, they still pose a threat to networks and computers.

Knowledge Check. Select the best answer.

Which cyber adversary collects intelligence for economic, political, or military gain?

- a. Nation States.
- b. Organized Crime.
- c. Terrorists.
- d. Hackers.

The correct answer is "Nation States." Nation States collect intelligence for economic, political, or military gain.

Activity. (Scroll Game) Screen 20.

Feedback: During peacetime, Nation States collect intelligence for political gain. Their cyber capabilities range from moderate to extremely skilled.

Feedback: Organized crime seeks huge profits through fraud. Their cyber capabilities range from moderate to extremely skilled.

Feedback: Terrorists use violence to cause uncertainty. Their cyber capabilities range from "script kiddie" to extremely skilled.

Feedback: Rival companies and foreign governments intend to gain an economic competitive edge in the market. Their cyber capabilities range from moderate to extremely skilled.

Feedback: Recreational Hackers seek notoriety. Their cyber capabilities range from "script kiddie" to extremely skilled. Click the right arrow to continue.

On Screen Text. Screen 21.

Summary.

By understanding the adversary's intent, and the inherent risks involved, you'll be better equipped to protect your information and avoid being compromised. Remember this information, and stay vigilant.

Nation States (during peacetime). During peacetime, Nation States collect intelligence for economic, political, and military gain.

Nation States (during times of crisis). During times of crisis, Nation States collect intelligence to attack mission-critical infrastructure systems.

Organized Crime. The intent of Organized Crime is to obtain huge profits through identity theft, extortion, corruption, and fraud.

Terrorists. Willing to die for their beliefs, terrorists seek to cause uncertainty, insecurity, fear, and apprehension.

Economic Competitors. Rival companies and foreign governments intend to gain an economic competitive edge in the market.

Recreational Hackers. Recreational Hackers seek notoriety and adventure.

Voice Over Script. Screen 21.

Now that we've identified the adversary, as well as his intent and capabilities, let's take a look at the vulnerabilities associated with mobile technology and the ways in which the adversary may exploit them.

Module 2.

On Screen Text. Screen 22.

Module 2: Mobile Technology

Voice Over Script. Screen 22.

In this module, we'll take an in-depth look at the vulnerabilities associated with portable devices and Bluetooth technology, as well as possible countermeasures available for continued data protection.

On Screen Text. Screen 23.

Portable Devices.

Simple Media: Requires a wired connection.

Smart Media: Transfers data via wired or non-cellular wireless connection.

On Screen Text. Screen 24.

Portable Devices. Risk.

There are multiple risks associated with the use of portable devices.

- Data loss.
- Data exposure.
- Network-based attacks.

Voice Over Script. Screen 24.

There are multiple risks associated with the use of portable devices.

Loss of the physical device increases the risk of data loss.

Public or third party access to sensitive information without consent increases the risk of data exposure.

Each time a portable device connects to any system, either directly or via the Internet, the risk of network-based attacks increases.

On Screen Text. Screen 25.

Portable Devices. Use countermeasures.

- Use a travel device when overseas.
- Don't use public Wi-Fi.
- Remove the battery when not in use.
- Disable Bluetooth, Wi-Fi, and GPS when not in use.
- Apply security and privacy settings.

Voice Over Script. Screen 25.

As organizations become increasingly scattered and more employees rely on portable and mobile devices, the potential risk for data loss grows.

Transferring files from a work device to a home computer not protected or maintained to company IT standards, using unsafe personal communications instead of proven corporate communications, talking about sensitive matters within hearing range of others, and failing to use a laptop privacy screen while working in public...these behaviors all invite information and data theft.

On Screen Text. Screen 26.

Portable Devices. Use countermeasures.

- Maintain physical control of the device.
- Vary when and where the device is used.

Voice Over Script. Screen 26.

Employees also fail to safeguard portable devices, such as laptop computers and storage devices, which can cause serious data loss if lost or stolen.

Additionally, the repeated use of a single device makes identifying and tracking potential targets easier for an adversary. Randomly deploying or distributing devices, swapping SIM cards, or changing service providers increases the difficulty of associating a particular device with a specific user.

On Screen Text. Screen 27.

Portable Devices. Indicators.

Indicators of malicious code include:

- Erratic device behavior.
- Unexplained windows.
- Dropped calls.
- Continuous radio activity indicator.
- Unexplained strong signal.

Voice Over Script. Screen 27.

Using text messages or emails, cyber adversaries may lure users to malicious sites or convince them to install malicious code on their portable devices.

Through this code, the adversary gains control of the device and may use it against other devices via Denial of Service attacks.

Attacks may also be able to turn infected cell phones and tablets into cyber-espionage devices, allowing adversaries to remotely track locations, download contact lists and personal

information, intercept and send messages, record conversations, and take pictures – all without the user knowing.

On Screen Text. Screen 28.

Cell Phones and Tablets.

Vulnerable to attacks initiated by text messages, emails, or via the Internet.

On Screen Text. Screen 29.

Cell Phones and Tablets. Use countermeasures.

- Maintain physical control.
- Limit posting your cell phone number and email address.
- Enable auto-lock, passcode lock, security settings, and encryption.
- Install security software and apply software updates.
- Only use applications from trusted sources.

Voice Over Script. Screen 29.

To reduce a cell phone or tablet's exposure to and risk of malware infection, employ these countermeasures.

On Screen Text. Screen 30.

Cell Phones and Tablets. Use countermeasures.

- Maintain the device's original operating system.
- Enable two-factor authentication when available.
- Restrict use of untrusted wireless networks.
- Configure web accounts to use secure connections.
- Turn off auto-fill in browser.

On Screen Text. Screen 31.

Cell Phones and Tablets. Use countermeasures.

- Set Bluetooth to non-discoverable.
- Disable Bluetooth when not in use.
- Limit Internet downloads; do not open anything unknown or unrequested.
- Remove unapproved devices from the workplace.

Knowledge Check. Select the best answer.

Cell phones and tablets are vulnerable to attacks initiated by text messages, emails, or the Internet.

- a. True.
- b. False.

The correct answer is "True." Cyber adversaries may use text messages or emails on cell phones and tablets to lure victims into clicking on malicious sites or installing malware.

On Screen Text. Screen 32.

Network Attacks.

Firmware vulnerabilities allow adversaries to access smart phones and networks.

Voice Over Script. Screen 32.

Adversaries may take advantage of well-publicized firmware bugs, which then allow them to spoof a particular cell phone tower or launch attacks via remote communications, such as text messaging.

On Screen Text. Screen 33.

Network Attacks. Use countermeasures.

- Apply latest software updates.
- Avoid using smart phones in areas where rogue base stations may exist.

Voice Over Script. Screen 33.

Although there is no foolproof way to protect a device against network attacks, employing the following countermeasures can limit the exposure and risk.

On Screen Text. Screen 34.

Malicious Apps.

Vulnerabilities in mobile apps could enable or allow malware to be executed.

Voice Over Script. Screen 34.

Mobile operating systems, like Android, are primary targets for malware attacks due to market shares and open source architecture.

Building a malicious app requires a low level of expertise; public app stores like Google Play are easily accessible, making them the best places to deploy malicious applications.

While many security firms focus on malware as the most serious threat mobile users face, the greatest danger actually comes from the sensitive data leaked by installed apps.

On Screen Text. Screen 35.

Malicious Apps. Surveillance.

Compromised devices may be used for:

- Audio.
- Camera.
- Call logs.
- Location.
- SMS messages.

Voice Over Script Screen 35.

An infected device's camera and audio may be accessed remotely and used to spy on the user. This surveillance – coupled with both location and messaging information gleaned from the device – places users in a potentially dangerous situation.

On Screen Text. Screen 36.

Malicious Apps. Data Theft.

Compromised devices may be used for:

- Account details.

- Contacts.
- Call logs.
- Phone number.
- Apps.
- International Mobile Equipment Identity (IMEI).

Voice Over Script. Screen 36.

Using malicious code, malware can steal all of the personal information stored on a smart phone, including the user's account details and contact list.

On Screen Text. Screen 37.

Malicious Apps. Impersonation.

Compromised devices may be used for:

- Redirecting SMS.
- Sending email messages.
- Posting to social media.

Voice Over Script. Screen 37.

Malware can also impersonate a user, using his or her device to send email messages from their accounts or post to social networking sites.

On Screen Text. Screen 38.

Malicious Apps. Botnet Activity.

Compromised devices may be used for:

- Creating Distributed Denial of Service (DDoS) attacks.
- Propagating click fraud.
- Sending premium rate SMS messages.

Voice Over Script. Screen 38.

Compromised devices may become part of a botnet, a group of Internet-connected computers, each maliciously taken over by malware. This botnet can be used to launch a Distributed Denial of Service attack, which renders a server or network unavailable for intended users.

Botnets may also run a background script that automatically clicks on paid ads to generate revenue or send premium rate messages from the user's account.

On Screen Text. Screen 39.

Malicious Apps. Financial.

Compromised devices may be used for:

- Stealing Transaction Authentication Numbers (TANs).
- Extorting via ransomware.
- Selling fake antivirus.
- Placing expensive calls.
- Sending premium rate SMS messages.

Voice Over Script. Screen 39.

To steal financial data, malware may capture the TANs used to authorize financial transactions, ransom the use of a computer system, or require users to pay for the simulated removal of malware – which actually introduces additional malware into the system.

Knowledge Check. Select the best answer.

The risk of downloading applications that are malicious is low due to the complexity of developing a malicious app.

- a. True.
- b. False.

The correct answer is “False.” Malicious apps are relatively cheap to produce and easy to develop.

Knowledge Check. Select the best answer.

Which of these below poses the greatest threat to computer users?

- a. Rogue cell towers.
- b. Falling prey to the Nigerian Prince scam.
- c. Sensitive data leaked by installed apps.
- d. Denial of Service.

The correct answer is “Sensitive data leaked by installed apps.” Installed apps may mine a user’s device and steal data from contact lists, locations, and personal information.

On Screen Text. Screen 40.

USB Drives.

Small, readily available, inexpensive, and extremely portable.

Associated Risks.

- Propagate malicious code.
- Infect devices directly during production.
- Data spillage.

Voice Over Script. Screen 40.

USB drives are easy to use and portable. They may be connected to or disconnected from a computer at any time. Upon connection, the operating system automatically activates the device and begins to communicate with it.

Keep in mind that unencrypted information stored on a USB drive can be accessed by anyone who uses that drive – including individuals who may find it if lost.

One option is for adversaries to use a USB drive to infect other computers. An adversary might infect a computer with malware that can detect when a USB drive is plugged into a computer. The malware then downloads malicious code on the drive. When the USB drive is plugged into another computer, the malware infects that computer.

Some adversaries have also targeted electronic devices directly, infecting items such as electronic picture frames and USB drives during production. When users buy the infected products and plug them into their computers, malware is installed on their computers.

In the classified space, using unclassified USB devices on classified systems may lead to data spillage and malware infection, which may fool a host into permitting the passage of malicious code.

On Screen Text. Screen 41.

Portable Media. Use countermeasures.

- Avoid accessing privileged accounts; instead, only login using a standard user account.
- Utilize passwords and encryption on USB devices.
- Employ an endpoint device control application to automatically keep certain types of devices from connecting to computer systems.
- Access the device in an isolated environment (virtual machine/sandbox).
- Make use of document viewers instead of full applications.
- Install antivirus software.
- Employ application whitelisting.

Voice Over Script. Screen 41.

Using the following countermeasures may reduce the risk of vulnerabilities to a portable device.

If an administrator has privileged account access, login as a standard user when using portable media to limit the risk of exposure.

Pay particular attention to applications and employ whitelisting, a technique that identifies those individuals and/or applications with a particular privilege, service, mobility, access, or recognition. Those on the whitelist are accepted, approved, recognized, and authorized access.

On Screen Text. Screen 42.

Portable Media. Use countermeasures.

- Sanitize files taken from removable media before distributing.
- Remove unnecessary media hardware devices from systems.
- Separate personal and business USB drives.
- Prevent unclassified devices from using classified hosts.

On Screen Text. Screen 43.

Portable Media. Use countermeasures.

- Avoid unknown USB devices.
- Disable AutoRun on the computer.
- Disable operating system support for unnecessary types of removable media.

On Screen Text. Screen 44.

Portable Media. Scenario.

A technology company provided complimentary USB drives at a security conference.

The USB devices contained malware that spread when the USB device was inserted into a Microsoft Windows workstation or server, via setup.exe and autorun.ini files that were automatically run.

Those who had their AutoRun disabled were not affected.

Knowledge Check. Select the best answer.

In regard to vulnerabilities, select the statement that best describes USB drives:

- a. Are a great choice for data transfer.
- b. Are guaranteed virus-free when new in box.
- c. Can propagate malicious code.

- d. Poses no threat to computer systems.

The correct answer is “Can propagate malicious code.” USB devices are risks for malware; they can infect computers with malicious code and may even come from the factory with malware already on them.

On Screen Text. Screen 45.

Bluetooth.

Short-range, low power, wireless technology.

Susceptible to a diverse set of security vulnerabilities.

Attacks involve:

- Identity detection.
- Location tracking.
- Denial of Service.
- Unintended control and access of data and voice channels.
- Unauthorized device control and data access.

Voice Over Script. Screen 45.

Standard commercial Bluetooth headsets are relatively insecure due to a lack of proper encryption and authentication methods.

Bluetooth headsets inherently support a set of powerful telephony commands, which can be used by an adversary to turn the device into a mobile bug that transmits everything it hears. This allows adversaries to not only eavesdrop on *that user's* conversations, but on the conversations of those individuals near or around him or her.

On Screen Text. Screen 46.

Bluetooth. Use countermeasures.

- Avoid standard, commercial Bluetooth headsets.
- Maintain physical control of devices at all times.
- Remove lost/stolen devices from paired device lists.
- Monitor devices and links for unauthorized Bluetooth activity.

Voice Over Script. Screen 46.

To protect a non-standard, commercial Bluetooth device and limit vulnerabilities, employ these countermeasures.

On Screen Text. Screen 47.

Bluetooth. Use countermeasures.

- Employ device firewalls, regularly patch Bluetooth devices, and keep antivirus software up to date.
- Utilize devices with low-power, Class 2 or 3 Bluetooth transceivers.
- Disable Bluetooth when not in use.
- Turn off discovery mode.

On Screen Text. Screen 48.

Bluetooth. Use countermeasures.

- Connect devices only if/when absolutely necessary.
- Pair Bluetooth devices in a secure area using long, randomly generated passkeys.
- Avoid entering Bluetooth passkeys when unexpectedly prompted for them.
- Keep devices as close together as possible when Bluetooth links are active.

Knowledge Check. Select the best answer.

In regard to vulnerabilities, select the statement that best describes Bluetooth technology:

- a. Can be secured and poses no risk.
- b. Is acceptable for sensitive communications.
- c. Should always be enabled.
- d. Is susceptible to a diverse set of security vulnerabilities.

The correct answer is “Is susceptible to a diverse set of security vulnerabilities.” Security vulnerabilities in Bluetooth devices may be exploited, turning them into mobile bugs that transmit every conversation within proximity of the device.

Activity. (Match Game) Screen 49.

Feedback: Loss of the physical device increases the risk of data loss. Maintain physical control to avoid.

Feedback: Cyber adversaries may lure users to malicious sites. Limit Internet downloads and do not open anything unknown or unrequested.

Feedback: An infected USB device can propagate malicious code when plugged into a computer. Disable AutoRun as a countermeasure.

Feedback: Disable Bluetooth devices when not in use to defeat the risk of enabling a mobile bugging device.

Feedback: The risk of network-based attacks increases every time a portable device connects to any system. Remove the battery when not in use.

Feedback: Disable your computer's AutoRun capability to mitigate risk of malicious code.

On Screen Text. Screen 50.

Summary

Apply countermeasures to limit the potential risks to critical information that have emerged from the ubiquitousness of portable devices in our daily lives.

Cell Phones/Tablets. Maintain physical control of your cell phone and tablet to decrease the risk of data loss.

USB Devices. USB devices may propagate malicious code; disable your computer's AutoRun capability to mitigate this risk.

Bluetooth Devices. Disable your Bluetooth device when not in use to decrease the risk of enabling a mobile bugging device.

Voice Over Script. Screen 50.

Mobile devices are a large part of society today and continue to demonstrate their usefulness and possibilities. With this in mind, let's take a look at the multiple possible sources of data leakage in the mobile environment and the countermeasures that can be employed to ensure the devices are locked down.

Module 3.

On Screen Text. Screen 51.

Module 3: Data Leakage in the Digital Age.

Voice Over Script. Screen 51.

In this module, we'll examine common computer vulnerabilities, the possibility of data leakage, the effects of risky behavior, and countermeasures to employ for continued data protection.

On Screen Text. Screen 52.

Data Leakage.

The unauthorized transmission of data (or information) to an external destination or recipient.

Voice Over Script. Screen 52.

While wireless devices and public hotspots increase productivity, and organizational networks facilitate communication, collaboration, and data access, these practices also introduce data to a broader, more vulnerable environment that is difficult to protect.

On Screen Text. Screen 53.

Data Leakage.

Personal Behaviors + Company Devices = Possibility of Data Leakage

Voice Over Script. Screen 53.

Adding to the complexity of how to best safeguard data is the thinning line between work life and personal life. Whether at work, on the road, or at home, employees continue to combine their personal behaviors with the use of company mobile phones, laptops, web applications, videos, and other social media – an equation that could lead to data leakage.

On Screen Text. Screen 54.

Data Leakage. Risky Behavior.

- Unauthorized use of applications.
- Misuse of information systems.
- Unauthorized physical and network access.
- Use of home computers for work.
- Misuse of passwords.

Voice Over Script. Screen 54.

Despite security policies, procedures, and tools currently in place, many employees engage in risky behavior – misuse of information systems or unauthorized applications, password sharing, unauthorized network access – that puts corporate and personal information at risk of loss or theft.

Employees working remotely may contribute to data leakage by transferring files between their work and home computers, or discussing sensitive work issues in public.

On Screen Text. Screen 55.

Data Leakage. Use countermeasures.

Avoid:

- Discussing sensitive information in public places.
- Sharing passwords.
- Using work devices for personal activities.
- Clicking on links within messages.
- Opening email attachments without verifying the sender.
- Using third-party application sites.

Encourage:

- Employing application whitelisting techniques.

Voice Over Script. Screen 55.

Data leakage may be inescapable, but employing countermeasures can curb both personal and corporate exposure and risk.

Pay particular attention to applications and employ whitelisting.

On Screen Text. Screen 56.

Data Leakage. Use countermeasures.

- Keep the device updated.
- Identify and protect critical information.
- Maintain physical security of devices.
- Log off or lock devices when not in use.
- Keep work and home devices separate.

On Screen Text. Screen 57.

Data Leakage. Use countermeasures.

Utilize:

- Data tracking.
- Data-at-rest encryption.
- Thin client remote access tools.
- Antivirus software.
- Strong passwords/passcodes.
- Privacy filters.
- Virtual Private Network (VPN).
- Security settings.
- Visitor control procedures.

Knowledge Check. Choose all that apply.

Employees engaging in risky behavior put corporate and personal information at risk.
Risky behavior includes:

- a. Misuse of information systems.
- b. Password sharing.
- c. Strong passwords.
- d. Unauthorized network access.

The correct answers are “Misuse of information systems, Password sharing, and Unauthorized network access.” Despite security policies, procedures, and tools currently in place, many employees engage in risky behavior—the misuse of information systems or unauthorized applications, password sharing, unauthorized network access— that puts corporate and personal information at risk of loss or theft.

Knowledge Check. Select the best answer.

Transferring files between work and home increases the likelihood of data leakage.

- a. True.
- b. False.

The correct answer is “True.” Keep home and work devices separate to limit the likelihood of data leakage.

Knowledge Check. Choose all that apply.

Data leakage countermeasures include:

- a. Smart phone as a data transfer device.
- b. Antivirus software.
- c. Privacy filters.
- d. Virtual Private Networks (VPN).

The correct answers are “Antivirus software, Privacy filters, and Virtual Private Networks (VPN).” Keeping software and firewalls updated, enabling privacy filters, using strong passwords, and logging on through a virtual private network will help protect against data leakage.

Knowledge Check. Select the best answer.

Data leakage refers only to computer systems.

- a. True.
- b. False.

The correct answer is “False.” Discussing sensitive information in public is also a form of data leakage.

Activity. (Scroll Game) Screen 58.

Feedback: Enforce visitor procedures to prevent unauthorized access, which can lead to data leakage.

Feedback: Utilize thin client remote access tools to counter data leakage when working on a personal device.

Feedback: Use privacy filters to avoid data leakage when using a computer in public. Click the right arrow to continue.

Feedback: Employ application white/blacklisting to prevent data loss through malware.

On Screen Text. Screen 59.

Summary.

Risky behavior can lead to computer vulnerabilities when accessing information systems. To stay compliant, and minimize risk, apply countermeasures to safeguard important data.

Use Thin Client Remote Access. Use thin client remote access instead of using personal devices for work.

Use a VPN. When working remotely, use a Virtual Private Network.

Use Privacy Filters. When working in public, use privacy filters.

Employ application white/blacklisting. To prevent data loss through malware, use application white/blacklisting.

Voice Over Script. Screen 59.

Data leakage is a scary prospect, but the mobile environment isn't the only place where it's possible. Let's take a look at other existing and emerging technologies that may also pose a great risk to our information.

Module 4.

On Screen Text. Screen 60.

Module 4: Yesterday and Tomorrow

Voice Over Script. Screen 60.

In this module, we'll discuss the vulnerabilities commonly associated with the ongoing use of social media, as well as the developing use of biometrics, the emerging Internet of Things, and advancements in cloud computing. We'll also take a look at countermeasures available for continued data protection.

On Screen Text. Screen 61.

Social Media.

Dependent on mobile and web-based technologies.

Offers powerful and covert means to target individuals.

Voice Over Script. Screen 61.

Social media encourages socialization and collaboration with not only friends and family, but also complete strangers. These interactions may leave the user vulnerable to potential social engineering attacks, as Nation States, hackers, and other adversaries grow increasingly adept at navigating cyberspace.

On Screen Text. Screen 62.

Social Media. Threats.

- Improperly administered sites.
- Weak Information Security controls.
- Malware.
- Malicious site redirection.

Voice Over Script. Screen 62.

There is a certain level of risk associated with accessing websites; this risk carries through social media usage.

Think of each site as a third-party platform through which savvy adversaries may aggregate information in order to gain access to private data. Security credentials may be compromised or personal preferences may be used to tailor spear phishing attacks.

On Screen Text. Screen 63.

Social Media. Threats.

- Social Engineering.
- Individual targeting (spear phishing, geo-location).
- Data aggregation.

On Screen Text. Screen 64.

Social Media. Use countermeasures.

- Enable privacy settings.
- Refrain from accepting friend requests from strangers.
- Disable location tracking.
- Assume all posts are public.
- Avoid online relationships that may reveal sensitive job information.

Voice Over Script. Screen 64.

The following countermeasures may help protect a user's social media presence and ensure that personal information remains private.

On Screen Text. Screen 65.

Social Media. Use countermeasures.

- Install trusted applications or software.
- Eliminate access to accounts from public computers or Wi-Fi hotspots.
- Avoid unknown links and files.
- Employ antivirus software and firewalls.

Knowledge Check. Choose all that apply.

Social media threats include:

- a. Social engineering.
- b. System hacking.
- c. Malware.
- d. Data aggregation.

The correct answers are "Social engineering, Malware, and Data aggregation." Adversaries may use compromised security credentials or social engineering tactics to gather personal preferences in an effort to tailor spear phishing attacks. Data aggregation may also be used in order to gain access to private information.

Knowledge Check. Select the best answer.

As long as privacy settings on social media sites are implemented, information is safe.

- a. True.
- b. False.

The correct answer is "False." Privacy settings help protect information. However, assume posts are public and act accordingly to avoid unnecessary threats.

On Screen Text. Screen 66.

Biometrics.

The statistical analysis and measurement of human traits or characteristics.

Vulnerabilities:

- Not changeable if biometric database is lost, stolen, or compromised.
- False acceptance.
- Spoofing.

Voice Over Script. Screen 66.

Biometrics are unique to an individual and do not require the memorization and use of a password or PIN.

At first glance, this uniqueness may suggest they are very secure; unfortunately, the lack of complete isolation leaves biometric systems exposed to the same risks as other networks and applications – as well as their own set of problems not shared by other systems.

On Screen Text. Screen 67.

Biometrics. Defeating biometric sensors.

- Fingerprint sensor.
- Facial recognition.
- Iris recognition.

Biometrics as part of a two-factor authentication process provides additional security.

Voice Over Script. Screen 67.

The reality is that biometric sensors alone do not provide sufficient security for high assurance applications simply because they can be beaten by a multitude of means.

Fake fingerprints can circumvent touch recognition systems; still photos and video of an authorized user defeat facial recognition systems; and a digital image of an authorized user's eye can fool an iris recognition system.

To significantly improve security benefits, users should employ biometrics as one component of a two-factor authentication process such as a password, PIN, or badge.

On Screen Text. Screen 68.

Biometrics. Defeating the iPhone TouchID:

- Several hours of work.
- Equipment worth thousands of dollars.
- Not an easy task.

Voice Over Script. Screen 68.

The Apple 5s TouchID technology was, in fact, defeated soon after it became available; however, the average user is unlikely to experience a hack of this type. It took several hours and required over a thousand dollars worth of equipment to actually complete the exploit.

Knowledge Check. Select the best answer.

Biometrics provide additional security as a component of a two-factor authentication process.

- a. True.
- b. False.

The correct answer is “True.” Biometrics, when used alone, can be defeated. To significantly improve security benefits, use biometrics as one component of a two-factor authentication process.

On Screen Text. Screen 69.

Internet of Things (IoT).

A network of everyday physical objects, such as washers/dryers that utilize Wi-Fi for remote monitoring, increasingly embedded with technology.

Collect and transmit data about their use and surroundings.

Voice Over Script. Screen 69.

In the new world of the Internet of Things – a network of everyday physical objects embedded with technology – the possibilities for data collection are endless, while the technology industry has only scratched the surface of what machine-to-machine interconnectivity may achieve.

On Screen Text. Screen 70.

Internet of Things (IoT). Vulnerabilities.

Enables data sharing about an individual’s habits, behaviors, and personal preferences.

Some of the main issues confronting the IoT are:

- Privacy and data protection.
- Autonomous communication.
- Traceability and unlawful profiling.
- Repurposing of data.
- Malicious attacks.

Voice Over Script. Screen 70.

IoT devices communicate with each other and transfer data without human interaction – a fact that many users may not be aware of. These data processing capabilities make security and privacy the primary weakness of IoT devices.

IoT devices continuously collect data, which – if paired with information gathered from other data sources – may reveal an individual’s habits, frequented locations, interests, and other personal information and preferences.

While this data could be repurposed for harmless targeted advertising, it could also be stolen and used for malicious attacks on security systems.

On Screen Text. Screen 71.

Internet of Things (IoT). Use countermeasures.

- Maintain an awareness of the IoT.
- Disable any geo- or activity-tracking capabilities that export data to external sites.
- Avoid linking IoT devices with social media and email accounts.
- Change default settings (e.g. SSID, password) whenever possible.

Voice Over Script. Screen 71.

Because the IoT is such a broad topic, specific mitigations are difficult to detail. However, in general, maintaining awareness of the risks associated with the devices they use provides all users with the foundation they need to protect themselves.

Knowledge Check. Choose all that apply.

Issues confronting the IoT include:

- a. Loss of privacy.
- b. Data protection.
- c. Social engineering.
- d. Repurposing of data.

The correct answers are “Loss of privacy, Data protection, and Repurposing of data.” Autonomous collection and data transmission decrease user privacy and make the data stored on IoT devices susceptible to loss and unintended or inappropriate use.

On Screen Text. Screen 72.

Cloud Computing.

Programs and applications running on connected servers.

Recent model for information technology implementation and management.

- Public: Third party.
- Private: Internally managed.
- Community: Shared by related organizations.
- Hybrid: Multiple cloud entities.

Voice Over Script. Screen 72.

A public cloud is owned and managed by a third party.

A private cloud is typically owned and managed internally, either on- or off-premises.

A community cloud is shared by related organizations with similar requirements.

A hybrid cloud is composed of two or more distinct cloud entities, coupled together.

On Screen Text. Screen 73.

Cloud Computing Vulnerabilities.

Security and privacy.

Providers and customer responsibilities.

Voice Over Script. Screen 73.

The idea of the cloud concerns some people, primarily the idea of placing their important data in another company’s hands. With the ability to log into the cloud from any location and access data and applications, users worry about the security and privacy of their information.

Cloud providers must ensure the security of their network and assert that their client’s data and applications are protected.

At the same time, cloud customers must ensure that their providers have taken the appropriate security measures to protect their information.

On Screen Text. Screen 74.

Cloud Computing. Use Countermeasures.

Private and community clouds have greater security measures and privacy controls than public and hybrid clouds.

When using a cloud service, enable authentication techniques and authorization format.

Voice Over Script. Screen 74.

Of the four types of cloud environments available, those customers at greatest risk of having their data compromised use public and hybrid clouds. Private and community cloud environments have greater security measures and privacy controls in place.

One way to protect privacy is through authentication techniques such as user names and passwords. Another approach is to employ an authorization format – each user can access only the data and applications relevant to his or her job.

Knowledge Check. Select the best answer.

Which cloud environments have the greatest security measures and privacy controls in place?

- a. Private and community.
- b. Public and community.
- c. Community and hybrid.
- d. Private and hybrid.

The correct answer is “Private and community.” The best security measures and privacy controls are provided by private or community cloud environments.

Activity. (Match Game) Screen 75.

Feedback: Enable privacy settings when using social media sites to decrease the risk of social engineering.

Feedback: Use two-factor authentication to provide additional security to biometrics.

Feedback: Pair with a second factor, such as a PIN or password, to enhance the security of biometrics.

Feedback: Disable activity tracking to avoid repurposing of data gleaned by the Internet of Things.

Feedback: Use private or community clouds to increase the security of your files in the cloud.

Feedback: Disable location services on your mobile devices to avoid geo-location.

On Screen Text. Screen 76.

Summary

Emerging technology has introduced a myriad of new threats for adversaries to target. Apply countermeasures to protect yourself and your information.

Social Media. Enable privacy settings when using social media sites to decrease the risk of social engineering.

Biometrics. Biometric enabled security is more effective when paired with a second factor such as a PIN, badge, or password.

Internet of Things. Disable activity tracking to avoid repurposing of data gleaned by the IoT.

Cloud Computing. Private and community clouds have increased security measures and privacy controls to increase the security of your files in the cloud.

Voice Over Script. Screen 76.

Your connection to the Internet makes you vulnerable, but the measures you take to protect yourself – and your information – help reduce your risk of data loss over time.

Advance to the next screen for an overview of what we covered throughout this course and to claim your certificate of completion.

On Screen Text. Screen 77.

Course Summary

- Cyber adversaries' intent and capabilities.
- Wireless and mobile devices and applications targeted for critical information.
- Computer vulnerabilities.
- Emerging technologies and associated vulnerabilities.

Voice Over Script. Screen 77.

Throughout this course, we provided practitioners with the information they need to maintain Operations Security in the face of the Cyber Threat.

We explored several common cyber adversaries, their intent, and their capabilities.

We also examined the vulnerabilities associated with wireless and portable devices, as well as Bluetooth technologies – and we detailed each technology's available countermeasures.

In addition, we discussed data leakage vulnerabilities within the mobile environment, as well as most appropriate countermeasures.

And finally, we looked at technologies of yesterday, today, and tomorrow, their associated vulnerabilities, and the potential countermeasures available.

On Screen Text. Screen 78.

Certificate

Certificate of Completion

The IOSS is pleased to award this certificate to _____ for the successful completion of the IOSS New Faces of Threats Training.

Date Completed: _____