SECURITY AWARENESS TRAINING

Montana Department of Justice

(Click anywhere to proceed)

NAVIGATING THE COURSE

- Once the audio for each screen is complete, click anywhere to progress to the next screen. *(Or select the Play button.)*
- Quiz questions require the correct answer to progress. Keep trying until you get the correct answer.
- When the course is complete a *Thank You* screen is displayed.
- Course controls are located along the bottom of your screen. If the controls are not displayed, adjust your window size (CTRL + or CTRL -) until they appear.

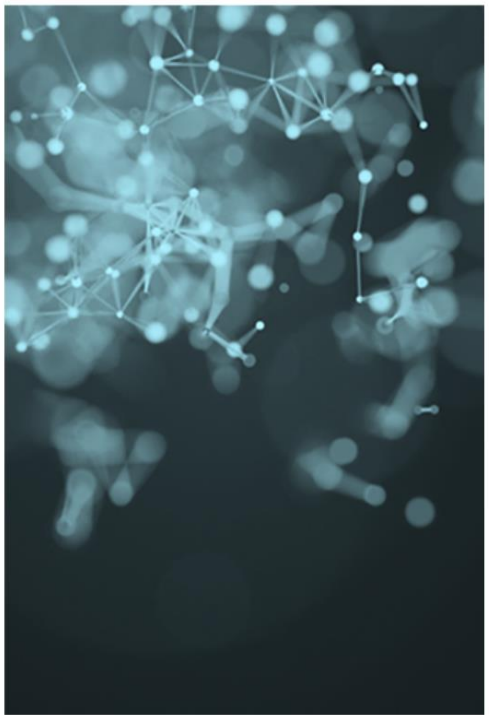
MANDATORY SECURITY AWARENESS TRAINING

This Security Awareness Training course is mandatory for all personnel who have access to Criminal Justice Information in any form.

This includes reading, writing, processing, or transmitting, as well as unescorted access to physically secure areas.

Security Awareness Training:

- Must be completed within six months of hire and
- Every two years after initial completion



Useful resources to accompany this course include:
CJIN User's Guide (CUG)
FBI CJIS Security Policy

HELPFUL HINTS

- This course does not require CJIN Access.
- This course should function on all modern browsers (Internet Explorer, Chrome, etc.).
- This course outlines the policies and procedures each employee and agency must follow to maintain compliance with the FBI Criminal Justice Information Services (CJIS) Security Policy.
- The CJIS Security Policy provides minimum security requirements associated with creation, viewing, modification, transmission, dissemination, storage, or destruction of Criminal Justice Information (CJI). Your agency may have further policies and procedures in addition to CJIS policy. Those policies may be stricter the FBI CJIS.

SECTION ONE:
CRIMINAL JUSTICE INFORMATION RESPONSIBILITIES

This section will cover the following topics:

- Criminal Justice Information (CJI) and the Criminal Justice Information Network (CJIN)
- Dissemination and Media Protection
- Physical and System Access
- Destruction, Noncompliance and Incident Reporting

It is your responsibility to protect CJI and ensure it is only being used for criminal justice or public safety purposes.

CRIMINAL JUSTICE INFORMATION

Criminal Justice Information (CJI) is data on people, vehicles, and property accessed in the performance of official criminal justice duties. In other words, data you need to do your job. This includes vehicle registration and drivers' license records, drivers' license photos, criminal history records, CJIN and NCIC hits on wanted persons, stolen vehicles, stolen property, etc.…

BASICALLY, IF YOU ACCESS INFORMATION THROUGH CJIN, IT IS CJI.

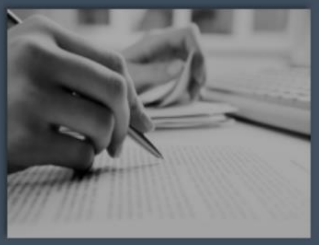
CJI is confidential and highly protected. It is only to be used for criminal justice and public safety purposes.

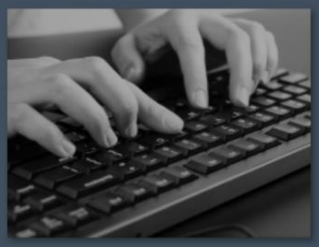
Whether you are in the vicinity of CJI, receive the printouts, or transmit the queries yourself, you are expected to secure the information and not expose it to threats.

MARKING AND HANDLING CJI

All CJI should be clearly labeled and kept in a physically secure area. This includes CJI printouts, any storage devices that contain CJI, and CJIN terminals.

- CJI processing devices should be positioned so the public cannot view them.
- Desktop monitors should be faced away from windows or public entrances.
- Mobile terminals should be positioned to prevent public viewing. They should be docked inside of a locked and secure patrol car.
- Use of security screens on monitors is encouraged.





FOR OFFICIAL USE ONLY (FOUO)

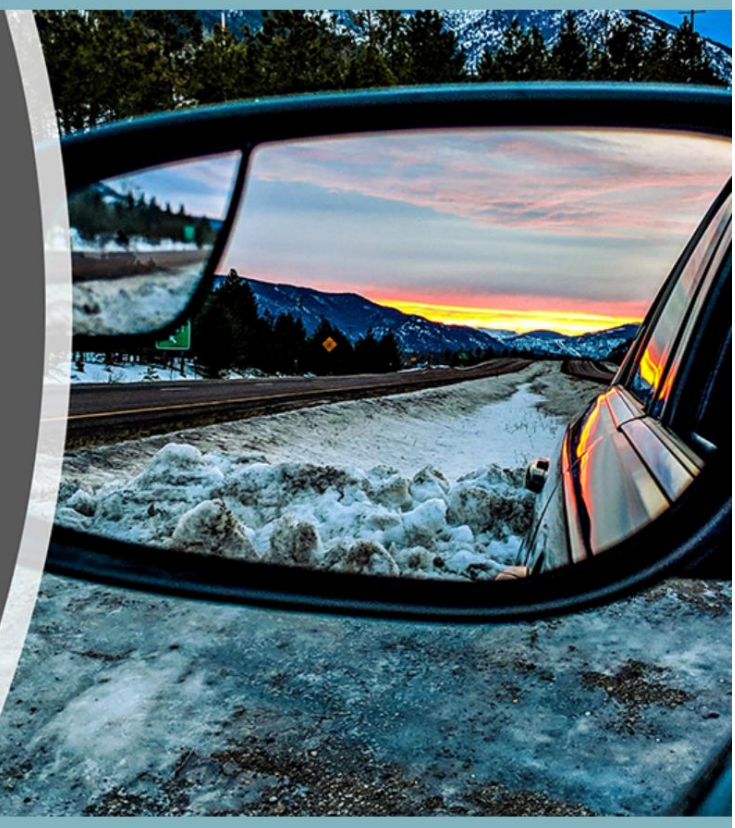
Any material marked "FOUO" should not be disclosed to anyone except criminal justice employees with a need to know. Your agency's network topology diagram is an example of a need-to-know document.

CAD SYSTEMS

Information that has been extracted and entered into your CAD or RMS is still CJI and requires protection.

DISSEMINATION

Dissemination is the communication or transfer of CJI. Sharing CJI is one of law enforcement's greatest tools and policies are in place to guarantee the protection of confidential information.



DISSEMINATION

PRIMARY DISSEMINATION

Primary dissemination is when a person requesting CJI is provided the CJI over the radio, by printout, or fax.

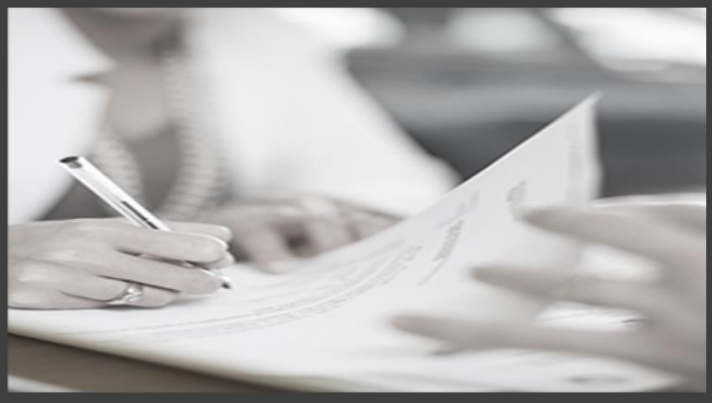
An example is when an officer requests a criminal history check from their dispatch center. Once the query is transmitted, the information is handed to the officer at the jail.

DISSEMINATION

SECONDARY DISSEMINATION

Secondary dissemination is when the initial recipient passes CJI to another authorized criminal justice professional. A secondary dissemination log must be kept by the originating agency any time secondary dissemination occurs.

An example is when your county attorney requests a copy of the criminal history before a court hearing. The officer takes the copy they were given from their dispatcher, fills out the secondary dissemination log and faxes it to the county attorney.



SOCIAL MEDIA

Social media can be a helpful investigative resource for law enforcement when used correctly. However, there are strict regulations for posting CJI on social media and other online forums.

- Photos, videos, or links containing CJI are protected and shall not be displayed on the internet.
- CJI printouts or any documents containing personally identifiable information (PII) should never be uploaded.

The only exception is a person's driver's license photo can be uploaded to social media if:

- They are a wanted person with a warrant on file.
- They are a missing person with a missing person report.

(This does not mean their entire driver's license return can be uploaded. Only the DL photo can be used under these circumstances.)

PERSONNEL ACCESS

Prior to granting unescorted access to a secure location or access to CJI, both fingerprint-based and name-based background checks are required. The results must be submitted to DOJ by the hiring agency. The results of the background check must be kept on file within your agency.

Anyone *escorted* inside a secure location, such as visitors, are not required to have background checks submitted or complete Security Awareness training. However, they must be escorted for the entirety of their visit and not allowed to view CJI. While not required, it is good practice to run background checks on visitors for the purpose of facility security.

UNESCORTED ACCESS

Unescorted access describes anyone who does not directly handle Criminal Justice Information for their job but is granted access to secure areas where CJI may be present. Example: janitorial staff, private contractors (painters, maintenance, phone/internet providers).

VISITORS

All secure areas must be clearly marked with an "Authorized Personnel Only" sign.
All visitor's identities must be verified before granting access to secure locations. Visitors must always be accompanied, and their identities must be monitored when entering and exiting secure areas. We suggest your agency has a visitor log to ensure documentation of who is in the building at any given time.
Example: Personal visitors, delivery persons

MEDIA PROTECTION

All CJI photos, documents and other media must be protected whether in digital or physical format and stored within physically secure locations. You and your agency must establish safeguards to ensure the security and confidentiality of the information.

****ALWAYS establish the person you are sending or giving CJI to is authorized to receive the information! ****

MOBILE TERMINALS




Never leave undocked mobile terminals unattended, especially in a public place such as a restaurant or café.

ENCRYPTED INFORMATION




Always encrypt CJI sent electronically before sharing with another agency. This means you cannot send CJI though your email unless your email is encrypted. Faxes sent over a telephone line are exempt from the encryption requirement, however, the fax must be in a secure area and the recipient must be authorized to receive the information.

CJI DOCUMENTS




Physical documents containing CJI should never be kept in public view such as by windows or on desks. While transporting physical documents ensure they are hidden from view in a folder or envelope during transport and only given to authorized individuals.

PORTABLE DEVICES




Always encrypt CJI before putting it on a device that could be lost or stolen such as a USB drive. Do not leave USB flash drives, CDs, hard drives, or other digital media storage devices containing CJI where the public can potentially have access to them.

LET'S TAKE A CLOSER LOOK AT HOW DIFFERENT CJIN DOCUMENT TYPES CAN BE TRANSMITTED.

CJI DOCUMENT TRANSMISSION

How should each document type be transmitted?

CRIMINAL HISTORY

COURT NOTIFI-CATION

MEMO

DRIVER'S HISTORY

(This slide does not have audio.) To complete this exercise, click on a document type then drag and drop it over the correct transmission type. Repeat until all the document types are matched with a transmission type. Select **Submit** to check if your answers are correct. If you need to try again, select **Reset** and the document types will return to where they started.

EMAIL

MEMO

COURT NOTIFI-CATION

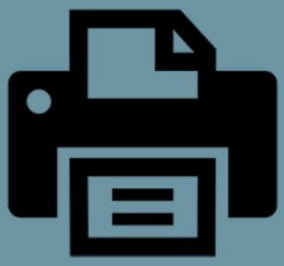
CRIMINAL HISTORY

DRIVER'S HISTORY

Reset

Undo

Submit



FAX

CJI DOCUMENT TRANSMISSION

Court Notifications and Memos can be sent via email.

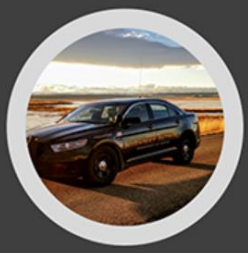
Driver's License images, Criminal History and Driver's History documents must be sent via fax.

COURT NOTIFI-CATION

MEMO

CRIMINAL HISTORY

DRIVER'S HISTORY



PASSWORDS

Passwords are required to access most applications and systems including the CJIS/CJIN system. This means in addition to your domain password (i.e. State or Windows) you will also need an additional password to access CJIS systems. This includes interface devices like mobile terminals, CJIN computers, and federal CJI kiosks.

Your password must be kept secure, changed frequently, and be unique to you.

NEVER share your password with anyone.
No IT professional will ever ask for your password!

CJIN PASSWORD REQUIREMENTS

Passwords accessing the CJIS/CJIN system must follow several rules.

Passwords must:

- **Be a minimum length of eight characters**
- **Not be the same as the User ID**
- **Expire within a maximum of 90 calendar days**
- **Not be identical to the previous ten passwords**
- **Not be transmitted outside of the secure location**
- **Not be displayed when entered**

It is recommended to keep different passwords for different systems and accounts. If your password is hacked or cracked, hackers will not have access to all your accounts because they have different passwords.

CREATING STRONG PASSWORDS

- Though CJIN only requires an eight-character password, a password of at least twelve characters is more secure.
- Consider using a passphrase instead of a password. Passphrases are a sequence of words or numbers which are easier to remember than a complex password. *An example is: Wel0veredautumnleave$*
- Develop mnemonics to remember your passwords.
- Use multi-factor authentication when available.
- Don't use passwords based on personal information that can be accessed or guessed.
- Don't use words exactly as the are found in the dictionary.
- Don't reuse passwords.
- Consider using a password manager to help you keep track of each password.

DESTRUCTION

- Once CJI is no longer needed, it must be destroyed. Physical documents must be shredded or incinerated, and digital files need to be overwritten.
- Shredding must be done by a crosscut shredder or a vendor approved by DOJ. If shredding is done by a third-party vendor, it must take place on site with authorized agency personnel present.

Keep the number of documents waiting to be destroyed to a minimum. Don't keep a to-be-shredded pile.

INCIDENT RESPONSE

DOJ Service Desk:
Phone 406.444.3993
Email DOJServiceDesk@mt.gov

DOJ Security Team:
Email DOJSecurity@mt.gov

You are in your facility everyday and know your surroundings better than anyone. If you see a suspicious person or activity, say something.

Immediately notify your Terminal Agency Coordinator (TAC) or supervisor of any possible security threat. Any form of security breach should be reported to DOJ IT department (contact information provided above) by your supervisor. If your supervisor or TAC is not available, follow your agency's policies and procedures.

Examples of possible threats include:

- Unauthorized personnel attempting to enter a secure area.
- Impersonating an officer or other employee to gain information or access to a secure area.
- Someone taking photos of CJI on their cell phone or other device.
- Eliciting information about an event or subject outside of their job description.
- CJI printouts found on the floor or outside of a secure area.

NONCOMPLIANCE

The serious consequences for misusing CJI and exposing state and federal systems to threats partially include:

- Violating public trust
- Loss of Credibility and respect for yourself and other members of the law enforcement community
- Termination of access
- Termination of employment
- Criminal prosecution (See MCA 45-7-601 below)
- Civil liability for your actions

MCA 45-7-601. Misuse of confidential criminal justice information.

A person commits the offense of misuse of confidential criminal justice information if the person is entitled to directly access the criminal justice information network and purposely or knowingly:

- *Accesses the criminal justice information network for personal use or financial gain; or*
- *Disseminates information accessed from the criminal justice information network to any person who is not authorized to receive confidential criminal justice information pursuant to 44-5-303.*

A person convicted of the offense of misuse of confidential criminal justice information shall be imprisoned in the county jail for a term not to exceed six months and be fined an amount not less than $500.

For purposes of this section, the following definitions apply:

"Confidential criminal justice information "has the meaning provided in 44-5-103.
"Criminal justice information network" has the meaning provided in 44-2-301.

Question 1- Multiple Choice

You notice someone that you know is not an employee lurking around your office and peering in windows right before you leave for break. What should you do?

- A) Immediately report this person to your TAC or supervisor.
- B) Immediately document this person in your suspicious person activity log.
- C) Go to lunch and see if they are still there when you return.
- D) Do nothing, there are always people around your office.

NOTE: Quiz questions and results do not have audio.

Submit

Question 1 of 20

Question 2-Multiple Choice

Who DOES NOT need a fingerprint and name-based background check and to be enrolled in Security Awareness Training before being allowed access to a restricted area where CJI is present?

- A) The facility's janitor who will be unescorted.
- B) The Police Chief's spouse visiting for lunch and will be escorted.
- C) The Terminal Agency Coordinator (TAC)
- D) The recently hired dispatcher

Submit

Question 2 of 20

Question 3-Multiple Choice

You find a printout containing CJI on an empty desk outside of the secure area of your building. What should you do with it?

- A) Put it inside the desk so it is not out in the open
- B) Leave it where you found it because someone will come back for it
- C) Immediately take it to your TAC or supervisor
- D) Keep it in case someone is looking for it

Submit

Question 3 of 20

Question 4-Multiple Choice

What is required if you provide CJI to an authorized agency outside your organization?

- A) It is never acceptable to give CJI to anyone outside of your agency.
- B) Whenever the person or property has left the jurisdiction of the originating agency, CJI should be transferred to the agency with jurisdiction
- C) CJI can be given to any other law enforcement agency if they request it if it is protected in transit
- D) A secondary dissemination log is completed by the originating agency and includes the name of the intended recipient of the information

Submit

Question 4 of 20

Question 5-True/False

Once CJI has been extracted and input into CAD system, it no longer needs to be secure and it is okay to share this information with anyone that request the information.

- A) True
- B) False

Submit

Question 5 of 20

Question 6-Multiple Choice

Why is it considered bad practice to use the same password for all the systems you access?

- A) Password requirements are different for different systems.
- B) If your password is ever cracked, the hackers can access all your accounts.
- C) Using the same password across systems is not a bad idea!
- D) Passwords must be changed every 60 days.

Submit

Question 6 of 20

Question 7- Multiple Choice

Which of the following is NOT a way to protect CJI?

- A) CJI must be labeled and kept in a physically secure, locked area when not in use.
- B) Mobile terminals should not be left unattended.
- C) Computer monitors should be positioned facing TOWARD windows or public access areas.
- D) When transporting physical CJI, it must be hidden from view and only given to authorized personnel.

Submit

SECTION TWO: TRENDING THEATS AND RISKS

This section will cover the following topics:

- Internal and External Threats
- Malware, Ransomware and Malicious Websites
- Social Engineering
- Phishing Emails
- Mobile and Rogue Devices

Since COVID-19 in early 2020 the U.S. FBI has reported a

300%

increase in reported cybercrimes.

INTERNAL AND EXTERNAL THREATS

Internal threats are vulnerabilities created by people within your agency such as:

- Snooping for non-work-related information
- Telling friends and family confidential work information
- Sharing information with the press or other organizations
- Stealing paperwork or USB drives
- Deliberately destroying or deleting information

External threats are vulnerabilities from outside your agency such as:

- Physically accessing secure areas where CJI is present.
- Email and phone scams
- Viruses and other malicious malware
- Hackers
- Members of the public viewing CJI purposefully or accidentally

THERE HAVE BEEN NUMEROUS TARGETED CYBER ATTACKS IN MONTANA

Beware!

The cyber security community is seeing an increase in targeted attacks nationwide against:

- City and County employees
- State Employees
- Schools and School Districts
- County Treasurers and staff
- Local Law Enforcement Agencies

MALWARE

Malware is the collective name for several malicious software variants, including viruses, ransomware and spyware. Shorthand for malicious software, malware typically consists of code developed by cyberattackers, designed to cause extensive damage to data and systems or to gain unauthorized access to a network.

Common ways malware gains access to devices are:

- Social Engineering
- Phishing emails
- Downloads from unsecure websites or email attachments
- Outdated antivirus definitions
- Use of default passwords on devices

MALICIOUS WEBSITES

Malicious websites are sites that attempt to install malware on your computer.

Malicious websites often mimic legitimate websites. Sometimes they'll ask you to install software that you appear to need to run a video or audio file.

It is for this reason internet use on CJIN and some agency computers is strictly regulated to work-related purposes only. This includes mobile terminals and interface devices. They all connect to CJIS and it is important to minimize risk whenever possible.

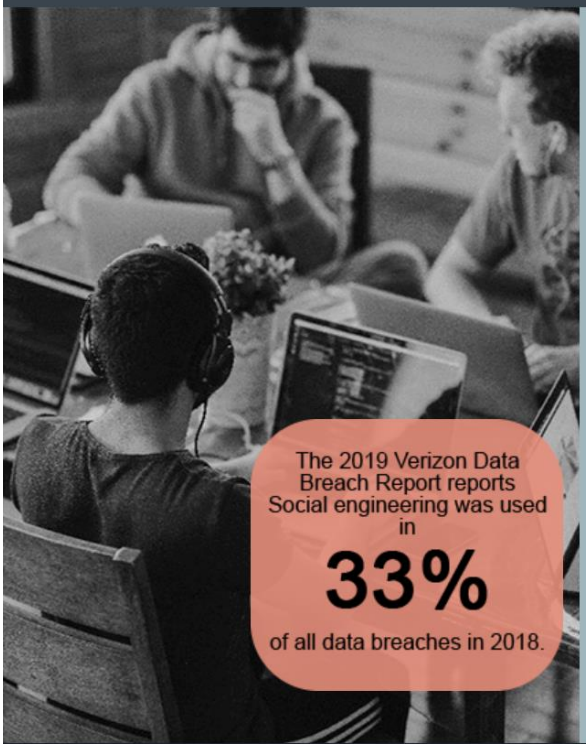
RANSOMWARE

Ransomware is a type of malware that infects your device (or your agency's devices), encrypts the data and prevents access to the system or files. Once attackers have locked down the data and/or device they demand payment to restore access or to not release your data.

There are several different ways that ransomware can infect your computer.

Malicious Spam is an unsolicited email which is used to deliver malware. The email might include booby-trapped attachments, such as PDFs or Word documents. It might also contain links to malicious websites. It often uses social engineering to trick users into opening attachments or clicking on links by appearing to be from a trusted institution such as the FBI/LEA or a friend.

SOCIAL ENGINEERING



Social engineering is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes. Criminals use social engineering tactics because it is usually easier to exploit your natural inclination to trust than it is to discover ways to hack your software.

Someone engaged in social engineering poses a threat to DOJ and CJI security. Social engineering is dangerous because it can be done remotely online or over the phone. Criminals do not need access to the victim's computer to gain access to confidential information. The digital aspect of social engineering makes it easier for an attacker to disguise themselves.

TYPES OF SOCIAL ENGINEERING

Always verify who you are speaking with whether in person, on the phone, or via email before sharing information. Ask for their contact information or call their employer to verify their employment. If they are there in person, you should ask to see their credentials.

TYPES OF SOCIAL ENGINEERING

Always verify who you are speaking with whether in person, on the phone, or via email before sharing information. Ask for their contact information or call their employer to verify their employment. If they are there in person, you should ask to see their credentials.

PHISHING seeks to obtain personal info using link shorteners or embedded links that redirect users to suspicious websites. For example, your agency uses Amazon to order some of the tactical gear for its officers. You receive an email from Amazon saying there is an issue with your account, and you need to use your log-in info to update your account. However, the link will take you to an unknown website.

TYPES OF SOCIAL ENGINEERING

Always verify who you are speaking with whether in person, on the phone, or via email before sharing information. Ask for their contact information or call their employer to verify their employment. If they are there in person, you should ask to see their credentials.

PRETEXTING focused on creating a fabricated scenario to build a false sense of trust with their victim to elicit information. *For example,* you receive a call from an unknown number. The person on the line says to you, “Hello, I am Detective Jones. Can you please send me criminal history on James Smith?” Without verifying his identity first, you could be victim to pretexting and compromising your agency.

TYPES OF SOCIAL ENGINEERING

Always verify who you are speaking with whether in person, on the phone, or via email before sharing information. Ask for their contact information or call their employer to verify their employment. If they are there in person, you should ask to see their credentials.

TAILGATING Also called “piggybacking” occurs when someone unauthorized follows an employee into a restricted area or uses their credentials to access websites or databases. For instance when you are entering the building after lunch and an unknown user follows you through the door before it closes.

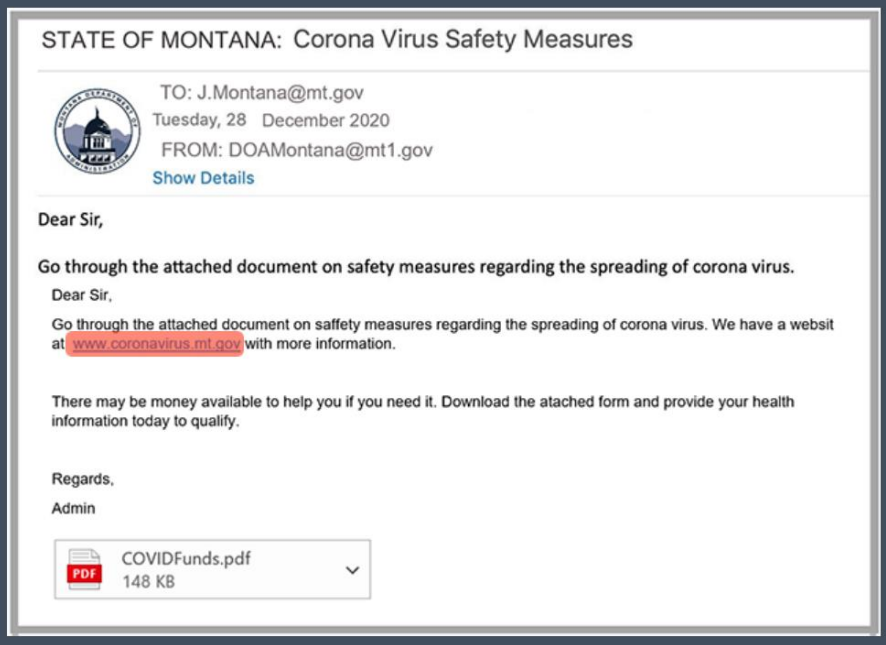
RECOMMENDATIONS

Steps you can take to protect your agency from social engineering include:

- Do not open emails from untrusted sources.
- If an offer from a stranger seems too good to be true, it probably is.
- Lock your computer or mobile terminal when not present.
- Ensure antivirus software is up-to-date.
- Know your agencies policies and procedures.
- If you see something, say something.

LET US TAKE A LOOK AT A FEW WAYS MALWARE AND SOCIAL ENGINEERING CAN BE USED TO HARM INDIVIDUALS AND ORGANIZATIONS.

PHISHING EMAILS



STATE OF MONTANA: Corona Virus Safety Measures

TO: J.Montana@mt.gov
Tuesday, 28 December 2020
FROM: DOAMontana@mt1.gov
Show Details

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.

Dear Sir,

Go through the attached document on saffety measures regarding the spreading of corona virus. We have a websit at www.coronavirus.mt.gov with more information.

There may be money available to help you if you need it. Download the atached form and provide your health information today to qualify.

Regards,

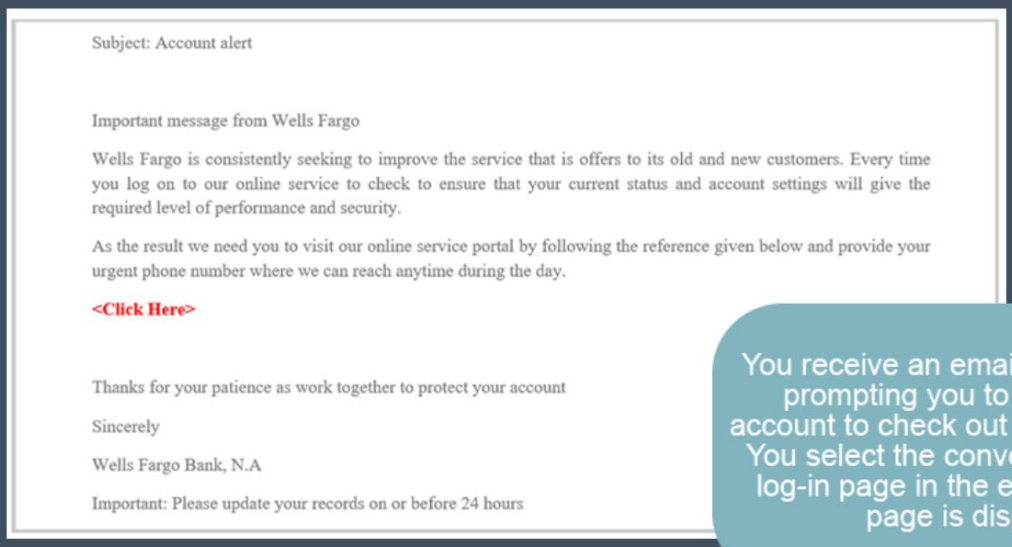
Admin

COVIDFunds.pdf
148 KB

You receive this email and are unsure if it is legitimate. To determine if it is a phishing email you should check the following:

When you hover over links and websites within an email, they should match what is displayed.

MALICIOUS WEBSITE



Subject: Account alert

Important message from Wells Fargo

Wells Fargo is consistently seeking to improve the service that is offers to its old and new customers. Every time you log on to our online service to check to ensure that your current status and account settings will give the required level of performance and security.

As the result we need you to visit our online service portal by following the reference given below and provide your urgent phone number where we can reach anytime during the day.

<Click Here>

Thanks for your patience as work together to protect your account

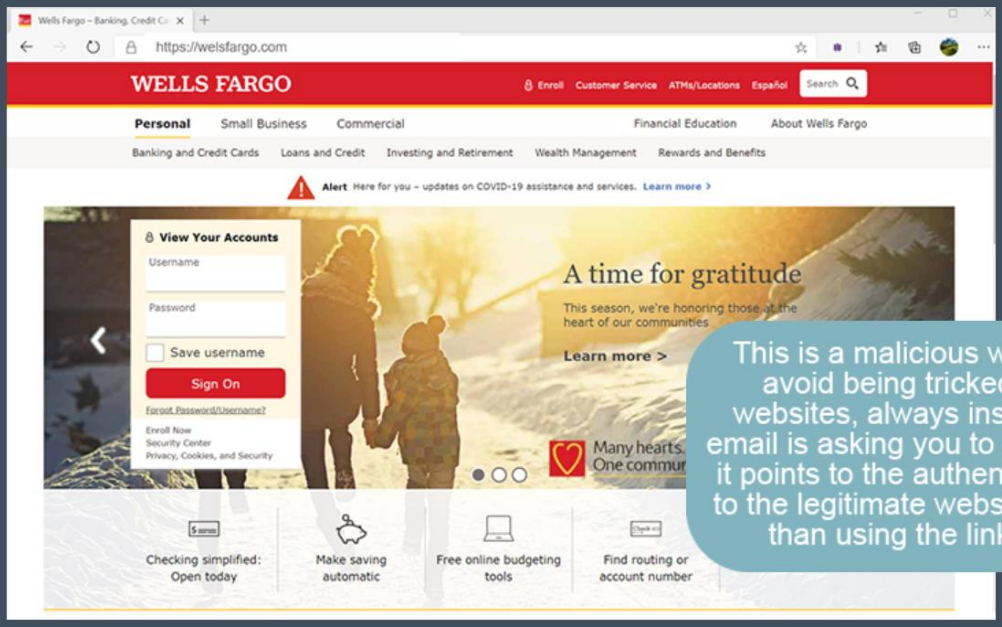
Sincerely

Wells Fargo Bank, N.A

Important: Please update your records on or before 24 hours

You receive an email from your bank prompting you to log in to your account to check out an urgent matter. You select the convenient link to the log-in page in the email and a web page is displayed.

MALICIOUS WEBSITE



This is a malicious website scam. To avoid being tricked by malicious websites, always inspect the link the email is asking you to click to make sure it points to the authentic domain. Or go to the legitimate website yourself rather than using the link in the email.

TECH SUPPORT SCAMS

You receive a call from Tech Support about a problem they see on your computer. You haven't contacted them nor have you had recent problems with your computer. The representative says she needs you to install a tool that will let her troubleshoot the program. She needs you to provide your email address so you can install the software using the link she provides.

TECH SUPPORT SCAMS

This is a version of a Tech Support scam. Tech support scams can be delivered a number of ways such as false contact information in emails/websites or through incoming phone calls.

Once in contact, a “technician” or “representative” will prompt you to install remote access or troubleshooting software.

ROGUE DEVICES

A rogue device is a wireless device that remains connected to a system but does not have permission to access and operate in a network. Rogue devices are malicious by nature. They exist for the sole purpose of stealing sensitive information like credit card numbers, passwords, and more. The best way to prevent rogue access and devices from connecting to your network is to scrutinize each device that joins your network as a potential threat.

- Also beware of connecting your devices to rogue Wi-Fi hotspots. They often mimic a legitimate hotspot provided by a business but allow attackers to eavesdrop from your device or even push malware out. Try to stay clear from public hotspots altogether or if you must, access Wi-Fi through VPN.

MOBILE DEVICES

Remember, hand-held devices often utilize Bluetooth, infrared, cellular, and other wireless protocols that are capable of joining networks or creating their own networks. These networks can place your devices at risk. Never connect to a network you don't 100% trust.

Much like our desktop and laptop terminals, mobile devices such as cell phones and tablets are also susceptible to attacks.

Some of the threats for mobile devices include:

- Loss, theft, or disposal
- Unauthorized access
- Malware
- Spam
- Electronic Eavesdropping
- Electronic tracking

Question 8-Multiple Choice

If you suspect a software install link you've been sent is untrustworthy and may be malicious in nature, what should you do?

- A) Forward it to your friends to see if they will install the software.
- B) Do not click on it, notify your supervisor or IT department.
- C) Click the link and see where it goes.
- D) Click the link but run a virus scan once the software is installed.

Submit

Question 9- Multiple Choice

Which one of the following is NOT an indicator of a possible phishing email?

- A) Messages sent via Reply All
- B) Embedded web links
- C) Suspicious attachments
- D) Generic greeting

Submit

Question 9 of 20

Question 10-Multiple Choice

What one of the following is an approach criminals use to gain access to a system through users?

- A) Through phone conferencing
- B) Through federal mail scams
- C) Through social engineering
- D) Through your family contacts

Submit

Question 10 of 20

Question 11-Matching Answers

Match the following terms with examples of the behavior.

Phishing

Pretexting

Tailgating

A) A stranger approaches you as you walk and follows you through a secure door.

B) You receive an invoice through email from what looks like a state employee's email address.

C) You receive a call from someone claiming to be an FBI agent asking for information.

Submit

Question 12- Multiple Choice

Malware does NOT gain access to devices through the following:

- A) Social Engineering
- B) Phishing emails
- C) Tailgating
- D) Use of default passwords on devices

Submit

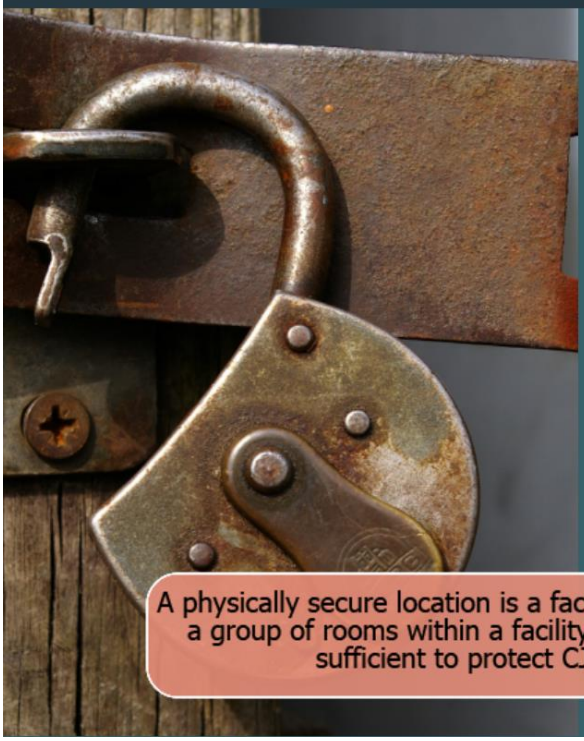
SECTION THREE: ADDITIONAL SECURITY MEASURES

This section will cover the following topics:

- Physical Security
- Security measures required for agencies and organizations
- Requirements for individuals

In 2019 it was reported
95%
of cybersecurity breaches were due to human error.

PHYSICAL SECURITY



- Physical Security of any device that handles CJI or DOJ information is one of the most critical facets of system security.
- All devices containing DOJ information and/or CJI must be stored in a physically secure location.
- For a mobile terminal that means locked and docked inside a patrol car that is also secured. For CJIN computers or servers, this means being in a locked area that is not accessible to the public or anyone not authorized to view CJI. For DOJ devices this means they are stored in a locked area or when traveling devices are with you or appropriately secured.

A physically secure location is a facility, a criminal justice conveyance, or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI, DOJ, and associated information systems.

The FBI has established eight criteria that define a physically secure area. The following screens explain each area type.

The explanations for each of the eight criteria will auto-play.
Click to proceed on the last screen as directed.

SECURITY PERIMETER

The perimeter of a physically secure location shall be prominently posted and separated from non-secure locations by physical controls.

PHYSICAL ACCESS CONTROL

The agency shall control all physical access points (except for those areas within the facility officially designated as publicly accessible) and shall verify individual access authorizations before granting access.

PHYSICAL ACCESS AUTHORIZATION

The agency shall develop and keep current a list of personnel with authorized access to the physically secure location (except for those areas within the permanent facility officially designated as publicly accessible) or shall issue credentials to authorized personnel.

MONITORING PHYSICAL ACCESS

The agency shall monitor physical access to the information system to detect and respond to physical security incidents.

ACCESS CONTROL FOR DISPLAY

The agency shall control physical access to information system devices that display CJI and shall position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.

VISITOR CONTROL

The agency shall control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible). The agency shall always escort visitors and monitor visitor activity.

DELIVERY AND REMOVAL

The agency shall authorize and control information system-related items entering and exiting the physically secure location.

ACCESS CONTROL FOR TRANSMISSION

The agency shall control physical access to information system distribution and transmission lines within the physically secure location.

MALICIOUS CODE PROTECTION

Effective patch management and antivirus software are required for DOJ and CJIS computers.

For patch management, local policies must include:

- Testing of appropriate patches before installation.
- Rollback capabilities when installing patches, updates, etc.
- Automatic updates without individual user intervention
- Centralized patch management program

Any patch requirements discovered during security assessments, continuous monitoring, or incident response activities need to be addressed expeditiously.

MALICIOUS CODE PROTECTION

System patches must be installed in a timely manner because patches are critical in fixing security vulnerabilities or other bugs.

Before installing system patches, your IT Department should install them on a test system, confirm they work, troubleshoot any potential issues, and finally install them on production systems.

The testing component is important because poorly designed or rushed patches can sometimes introduce new problems.

MALICIOUS CODE PROTECTION

Viruses, Trojan Horses, and other malicious codes help hackers gain access to our systems.

Your agency must have malicious code protection that includes automatic updates for all systems with internet access. Software companies often include security updates when they push through updates. By installing updates, you ensure your computer and systems have the most recent patches and fixes to avoid malicious code.

When your IT Department pushes updates to your computer, don't delay installing them.

DATA BACKUP

There are two approaches to data backup and storage; centralized or decentralized.

- A centralized approach replicates data from remote sites and sends it over a network to a main (centralized) location for storage. This type of backup can be used to automate backups at remote sites.
- A decentralized approach involves data being stored on multiple computers housed by participants cooperating on a network. One example of this is cloud storage.

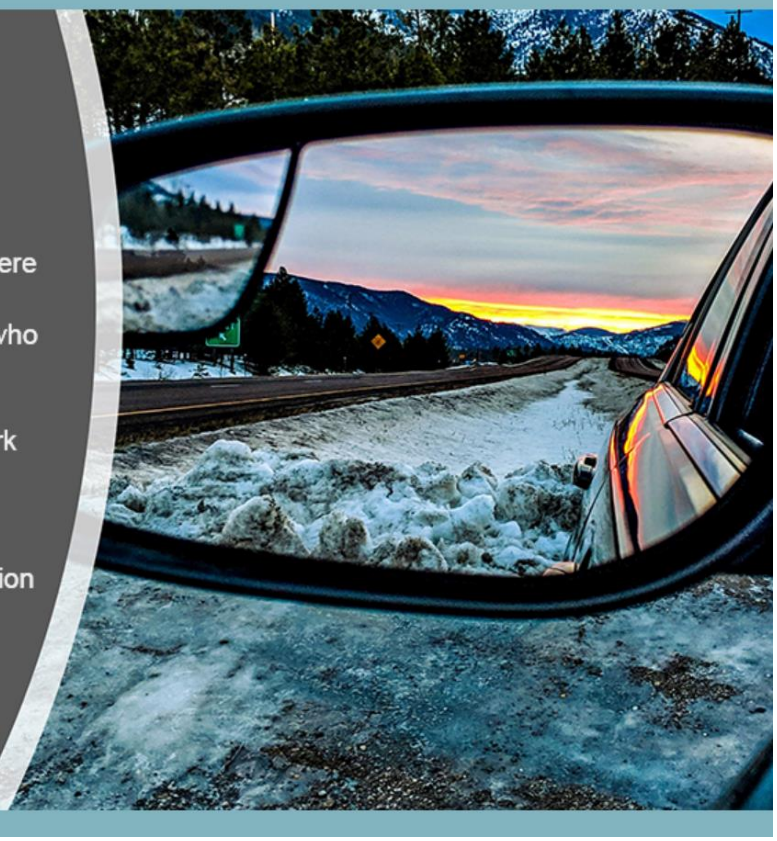
Regardless of which approach your agency takes, data storage must comply with FBI CJIS policy.

NETWORK INFRASTRUCTURE

Network infrastructure is another key area where systems need to remain secure. This not only means physical and virtual security, but also who is accessing the system and from where.

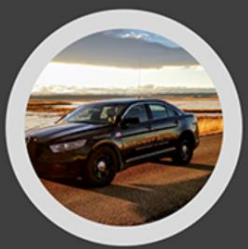
Some of the requirements for a secure network infrastructure include:

- Controlling login information
- Enforcing regular password changes
- Two-factor (or multi-factor) authentication when possible
- Regular virus and malware scanning
- Patches and updates when available
- Robust firewall system



DESKTOP SECURITY

- Our computers enable us to receive protected CJI in a matter of seconds. It is important to keep that information secure, even in an office environment.
- FBI CJIS policy states a computer on the system must have a 30-minute session lock. This means the computer locks after 30 minutes of inactivity. System locks need to be in place to prevent inadvertent viewing when your device is unattended. One of the most basic types of screen lock is the screensaver. Enabling screensavers help prevent any unauthorized viewing by replacing the computer screen on an idle computer to a blank or moving image.
- In addition to a screensaver, it's a good practice to use a privacy screen. Privacy screens are polarized sheets of plastic that prevent visibility from angles other than straight on. By utilizing a privacy screen, "shoulder surfing" and wandering eyes can be avoided. Only authorized personnel should be able to view your screen.



INFORMATION PROTECTION

It is your responsibility to protect sensitive information. Remember this information can be stored in your CAD/RMS system, on archive/backup software, and portable media.

- Any devices or systems that store sensitive information must be kept in a physically secure location. This can include portable hard drives, flash drives, CDs, DVDs, or memory cards.
- Your responsibility does not end until the sensitive information is disposed of properly. For physical media, this means data destruction. For digital media, this will be sanitation.
- Sanitation is either overwriting at least three times or degaussing the digital media prior to disposal or reuse.

PERSONAL EQUIPMENT

- Any personal equipment shall not be authorized to access, process, store, or transmit CJI unless the agency has established specific terms, conditions, and policy for their usage.
- This also applies for personal equipment such as flash drives, hard drives, or CDs/DVDs. If you are going to use these types of equipment, ensure you have prior approval.

DISPOSAL

Any inoperable digital media, such as a broken hard drive, needs to be destroyed (cut up, shredded, etc.)

Electronic Media:

- Your agency is responsible for maintaining written documentation of the steps taken to sanitize or destroy electronic media. This process needs to be witnessed or carried out by authorized personnel.

Physical Media:

- Physical media needs to be securely disposed of when it is no longer required. Formal procedures are necessary to minimize the risk of sensitive information getting into the wrong hands.
- Physical media needs to be either shredded or incinerated. It is the agency's responsibility to ensure the destruction is witnessed or carried out by authorized personnel.

WORKING FROM HOME

The good security habits listed below are essential to keep yourself and your agency safe while you are working from home.

- Use a VPN connection *(if available)*.
- Ensure your home router has a strong password *(not the default one)*. **Your internet provider can help you change the password if needed.
- Install software updates as soon as you are prompted.
- Only use your work computer for work related purposes.
- Ensure your work computer is only being used by you by keeping it locked while not in use.

INDIVIDUAL ACCOUNTABILITY

Individual Accountability means you are accountable for all your actions. You are expected to perform queries and use the system in accordance with FBI CJIS, CJIN, DOJ and your own agency's policies. Every query you make in the system is recorded and can be audited at any time.

ACKNOWLEDGEMENT STATEMENTS

For example, any system connected to CJIN must have users acknowledge the following:

- The user is accessing a restricted information system.
- System usage may be monitored, recorded, and subject to audit.
- Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.
- Use of the system indicates consent to monitoring and recording.

ACKNOWLEDGEMENT STATEMENTS

- Acknowledgment statements are used to document and acknowledge the receipt and understanding of information. We see these statements with HR forms, privacy notices, and even computer programs.
- These are statements that explain the rules of the system you are accessing. Many of the statements include why you have access to the systems and data that you do, what the purpose of the data is, and the consequences of misusing the privileges given.
- They will also mention not using the system for any kind of personal use or gain and keeping your password to yourself.
- Every time you select “OK” or “Acknowledge” you are agreeing to the conditions set forth by the statement.

Question 13-Multiple Choice

Why is it important to update your computer software whenever your IT department pushes through updates?

- A) Operating updated software always makes your computer run faster
- B) Updates and patches frequently contain security updates
- C) It is not important to update your software
- D) The system will never send pop ups once you've updated your software.

Submit

Question 13 of 20

Question 14-True/False

System access is given on a "need to know/need to share" basis meaning you are not given access to systems you don't need to access for your job duties.

- A) True
- B) False

Submit

Question 14 of 20

Question 15-Multiple Choice

Which is NOT a way to protect the data on your computer?

- A) Screen-savers/Screen lock
- B) Privacy Screens
- C) Storing your computer in a secure location, otherwise known as physical security.
- D) Monitor dimness setting at 15%

Submit

Question 15 of 20

Question 16-True/False

If a mobile terminal is interfaced with FBI CJIS, internet use on the computer is only permitted for work related purposes.

- A) True
- B) False

Submit

Question 16 of 20

Question 17-Multiple Choice

Your responsibility in handling sensitive Criminal Justice Information does not end until:

- A) The sensitive information is disposed of properly.
- B) Your responsibility doesn't end, it's a lifelong commitment.
- C) You turn the data over to someone else.
- D) You are finished accessing the data

Submit

Question 17 of 20

Question 18-True/False

If a visitor signs into the visitation log, they are free to roam all areas of the building including the secure areas because their visit is documented.

- A) True
- B) False

Submit

Question 18 of 20

Question 19-Multiple Choice

What is NOT one of the requirements for a secure network infrastructure?

- A) Robust firewall system
- B) Multi-factor authentication when necessary
- C) A notebook containing written IP addresses for your network
- D) Regular virus and malware scanning

Submit

Question 19 of 20

Question 20-Multiple Choice

Individual Accountability is defined as:

- A) Document and acknowledge the receipt of information
- B) Unsolicited messages, usually advertisements
- C) A place with controls sufficient to protect CJI
- D) You are accountable for all your actions.

Submit

Question 20 of 20

SECTION FOUR: CONCLUSION

This section will cover the following topics:

- Final comments
- Quiz Results

Security Awareness Training can reduce the risk of social engineered cyber threats by up to

70%

IN CONCLUSION

- DO NOT click on any links you are not familiar with or run any programs not authorized by your IT Department. Viruses and Trojan horses cannot work if you don't run their programs!
- If you are not sure about a program or link, call your supervisor or IT Department before downloading or installing it.
- It is your responsibility to protect CJI, PII and confidential information to ensure it is only being used for criminal justice or public safety purposes.
- If you suspect someone abusing CJI or not using it for the intended purpose, report it to your TAC or supervisor immediately.

Quiz Results

NOTE: Quiz questions and results do not have audio.

You Scored:	190
Maximum Score:	200
Correct Questions:	19
Accuracy:	95%

Continue

Be vigilant! Scrutinize your emails, attachments and downloads. Be aware of your surroundings to protect yourself, your agency and MT DOJ.

- Minimize the websites you visit to keep our network safe.
- Human intelligence and comprehension are the best defense against phishing attacks.

If you ever suspect that your computer or the system has been compromised, immediately contact your TAC, your supervisor and MT DOJ's Security Office (406-444-3993 or DOJSecurity@mt.gov).


You have completed
Security Awareness Training!
Thank You
Photo credits include:
Montana Highway Patrol, Department of Justice website, Lt. J.C. Denton, Trooper James Beck, Trooper Danny Sons, Trooper Seth Adams, Trooper Reisinger, Trooper Lane Knows His Gun, Trooper Cherie Lofton, Yellowstone Co. Sheriffs Office, Trooper Kurt Miller and Trooper Josh Nanna.