



TAC Conference 2025

Training

Security Awareness



Overview

Why train security awareness?

- What is required?
- Can I use other training to fulfill SAT?

Role Based Training

- Who fits into these roles?
- What do I cover?

Tracking training

Training ideas

Updating training materials

Why train security awareness?



Why train security awareness?

- To ensure that all users and non-users with authorized access to CJI be made aware of their individual responsibilities and expected behavior when accessing CJI and the system which process CJI
 - Insider threat
 - Social engineering and mining

Why train security awareness?

- To ensure that all users and non-users with authorized access to CJI be made aware of their individual responsibilities and expected behavior when accessing CJI and the system which process CJI
 - **Insider threat**
 - Can include behaviors such as inordinate, long-term job dissatisfaction; attempts to gain access to information not required for job performance; unexplained access to financial resources; bullying or harassment of fellow employees; workplace violence; and other serious violations of policies, procedures, directives, regulations, rules, or practices

Why train security awareness?

- To ensure that all users and non-users with authorized access to CJI be made aware of their individual responsibilities and expected behavior when accessing CJI and the system which process CJI
 - Insider threat
 - **Social engineering and mining**
 - An attempt to trick an individual into revealing information or taking an action that can be used to breach, compromise, or otherwise adversely impact a system. Social engineering includes phishing, pretexting, impersonation, baiting, quid pro quo, thread-jacking, social media exploitation, and tailgating. Social mining is an attempt to gather information about the organization that may be used to support future attacks

Can I use agency required SA fulfill this requirement?

- Can be used for some topics
 - Phishing
 - Baiting
 - Piggybacking
 - Workplace security, etc.
- SAT should be focused on security awareness as it relates to CJIS data
 - Handling CJIS data (Printed, electronic, etc.)
 - Baiting in regards to CJIS data
 - Sending CJIS data in a secure email

CJIS Data

- Criminal Justice Information is the term used to refer to all of the FBI and BCI CJIS provided data necessary for the administration of criminal justice
- Includes, but not limited to
 - Biometric Data
 - Identity History Data
 - Biographic Data
 - Property Data
 - Case/Incident History
 - Motor Vehicle
 - Driver License
 - Warrant
 - Protective Order
 - Criminal History


How often do I train SAT?

- As part of initial training for new users prior to accessing CJIS information and annually thereafter; and
- When required by system changes or within 30 days of any security event for individuals involved in the event

Role Based Training



Role Based Training




All individuals with
unescorted access to
a physically secure
location



General Users




Privileged Users



Organizational
Personnel with
Security
Responsibilities

Role Based Training



**All individuals with
unescorted access to
a physically secure
location**



General Users



Privileged Users



Organizational
Personnel with
Security
Responsibilities

Who

- BCI term
 - Non-users
- Custodial staff, maintenance staff, etc.



Minimum Required Training

- Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information Penalties
- Reporting Security Events
- Incident Response Training
- System Use Notification
- Physical Access Authorizations
- Physical Access Control
- Monitoring Physical Access
- Visitor Control
- Personnel Sanctions



Training Example



BCI Security Awareness Training

User Security



User Security


Fingerprint-based background checks for all:

- **Users**
 - Anyone who logs into UCJIS directly
- **Non-access Users**
 - Anyone who receives information indirectly from UCJIS
- **Non-Users**
 - Anyone with unescorted access that does not receive or access UCJIS information




User Security

- All BCI employees are required to have a User Security Agreement and User Training and Testing Agreement on file



UCJIS USER SECURITY AGREEMENT



Per Utah Administrative Rule R722-900, a **USER** means a person working for or with an agency who has direct access to UCJIS or a **NON-ACCESS USER** who obtains UCJIS records from a person who has direct access.

UCJIS USER SECURITY STATEMENT

Dissemination, Privacy, and Security of Information: All of the information acquired from any file accessed in UCJIS, which includes ULEISA, the Public Safety Alerts and Notifications System (PSANS), and NDex, is governed by regulations and policies of the FBI and the State of Utah. Dissemination, along with the privacy and security of any information acquired from any file in UCJIS, is for criminal justice purposes only. This information should be used for criminal justice purposes and criminal justice employment only. Printed copies must be destroyed by shredding or burning when no longer needed. Per the Administrative Office of the Courts, local and state records are maintained in a secure manner and are not to be released to the public without a court order or record summary.

Misuse of UCJIS information: Violation of this agreement may result in civil and/or criminal prosecution of the person who misuses the information. BCI maintains an automated system that monitors for unauthorized access to UCJIS information. Any unauthorized access could be considered misuse. Utah Code Ann. § 33-37(12) (a) It is a class B misdemeanor for a person to knowingly or intentionally disseminate a record created, maintained, or to which access is granted by statute, rule, regulation, or policy of a governmental entity.

User ID: Each UCJIS user must have a unique User ID. Each user will be held accountable for the use of their User ID.

Criminal Background Checks: All users must have a current criminal background check, a Utah Concealed Firearm Permit (CFP), must be a resident of Utah, and must not be prohibited from possessing a firearm to access UCJIS information or receiving UCJIS information. The criminal background check contains both a name and fingerprint check. The criminal background check must be submitted to the Utah Crime Information System (UCIS) Back System retains prints for the purpose of future criminal background check submissions. The existence of a criminal conviction may result in loss of access to UCJIS or UCJIS information.

UCJIS USER SECURITY AGREEMENT


I, _____, understand that I must abide by this agreement to use UCJIS.

Signature: _____


Date: _____ Agency ORI: _____

This agreement must be signed prior to access to UCJIS. This form does not constitute a contract. Please submit this agreement to your supervisor for review and signature.

Revised March 2024



UCJIS USER TRAINING AND TESTING AGREEMENT



for _____

USER OR NON-ACCESS USER (Please Print) _____ USER OR NON-ACCESS USER ID _____

This agreement must be signed and submitted to BCI after the completion of the user or non-access user's initial training and testing and after each biennial training and testing.

UTAH ADMINISTRATIVE RULE R722-900 DEFINITIONS:

USER: a person working for or with an agency who has direct access to UCJIS.

NON-ACCESS USER: a person working for or with an agency who asks for and/or receives UCJIS records.

REQUIRED TRAINING OF EACH USER AND NON-ACCESS USER:

RESTRICTIONS ON ACCESS, USE, AND CONTENT OF UCJIS RECORDS: UTAH CODE 53-10-108 ☐

DISSEMINATION, PRIVACY, AND SECURITY OF UCJIS INFORMATION ☐

UCJIS REQUIRED SECURITY AWARENESS TRAINING ☐

REQUIRED TRAINING AND TESTING FOR USER:

BCI MANUALS AND/OR NCIC MANUALS: LOCATION AND USAGE ☐

PLEASE CHECK THE FILES THE USER WAS TRAINED AND TESTED ON:

DLD ☐ NLETS ☐ MVD ☐ III ☐

UCH ☐ NCIC Inquiry ☐ NCIC Entry ☐ SWW/PO ☐

UCJIS CERTIFICATION: The TAC has updated the CERT transaction: Yes ☐ No ☐

This certifies that this user or non-access user has passed all of the required training and proficiency testing to be able to access UCJIS information.

UCJIS USER AND NON-ACCESS USER AGREEMENT

I certify that by signing this document that I have been trained and/or proficiency tested according to the procedure set by my agency, BCI, and CJIS. I accept that I will be held accountable for any information accessed under my user ID. I understand per Utah Code Annotated 53-10-108 (12)(a), it is a class B misdemeanor for a person to knowingly or intentionally access, use, disclose, or disseminate a record created, maintained, or to which access is granted by BCI or any information contained in a record created, maintained, or to which access is granted by BCI for a purpose prohibited or not permitted by statute, rule, regulation, or policy of a governmental entity.

USER OR NON-ACCESS USER'S SIGNATURE _____

TAC SIGNATURE _____ DATE SIGNED BY TAC _____



AGENCY _____ ORI _____

Please submit to your BCI Field Services representative or bcifs@utah.gov per Utah Administrative Rule R722-900-4

Revised May 2024

User Security Agreement

- The User Security Agreement covers:
 - Dissemination
 - Security
 - Privacy
 - Misuse
 - User ID
 - Background check
 - FBI Rap Back Fingerprints



UCJIS USER SECURITY AGREEMENT

Per Utah Administrative Rule R722-900, a **USER** means a person working for or with an agency who has direct access to UCJIS or a **NON-ACCESS USER** who obtains UCJIS records from a person who has direct access.

UCJIS USER SECURITY STATEMENT

Dissemination, Privacy, and Security of Information: All of the information acquired from any file accessed in UCJIS, which includes ULEISA, the Public Safety Alerts and Notifications System (PSANS), and NDex, is governed by regulations and policies of the FBI and the State of Utah. Dissemination, along with the privacy and security of any information acquired from any file in UCJIS, is for criminal justice purposes only. This information should be used for criminal justice purposes and criminal justice employment only. Printed copies must be destroyed by shredding or burning when no longer needed. Per the Administrative Office of the Courts, local agencies may NOT generate a hard copy of a juvenile's rap sheet or record summary.

Misuse of UCJIS information: Violation of dissemination, privacy, or security regulations may result in civil and/or criminal prosecution of the person(s) involved and loss of state computer access for the user and his/her agency. BCI maintains an automated dissemination log of all UCJIS file transactions to help ensure this information is being accessed for authorized purposes. Any unauthorized request or receipt of this information could be considered misuse. Utah Code Annotated 53-10-108(12) (a) states:

(12) (a) It is a class B misdemeanor for a person to knowingly or intentionally access, use, disclose, or disseminate a record created, maintained, or to which access is granted by BCI or any information contained in a record created, maintained, or to which access is granted by BCI for a purpose prohibited or not permitted by statute, rule, regulation, or policy of a governmental entity.

User ID: Each UCJIS user must have his/her own user ID that must never be shared even for training purposes. Each user will be held accountable for each transaction in UCJIS under his/her user ID.

Criminal Background Checks: All UCJIS users, including those who are POST certified or who have a Utah Concealed Firearm Permit (CFP), must undergo a criminal background check prior to having direct access to UCJIS information or receiving UCJIS information from a user with direct access. The criminal background check contains both a name and fingerprint search of UCJIS files and the FBI RAP Back System. The FBI RAP Back System retains prints for the purpose of being searched by future submissions including latent fingerprint submissions. The existence of a criminal conviction, outstanding warrant, or a new criminal arrest may result in loss of access to UCJIS or UCJIS information.

UCJIS USER SECURITY AGREEMENT

I, _____, have read and accepted the *UCJIS User Security Statement* and understand that I must abide by this agreement to have access to any information acquired through UCJIS.

Signature: _____ User ID: _____

Date: _____ Agency ORI: _____ Agency Name: _____

This agreement must be signed prior to accessing UCJIS or receiving any UCJIS information.
This form does not need to be signed for biennial re-certification.
Please submit this agreement to your BCI Field Services representative or bcifs@utah.gov per Utah Administrative Rule R722-900-4.

Revised March 2024

Workplace & Telework Work Station Security

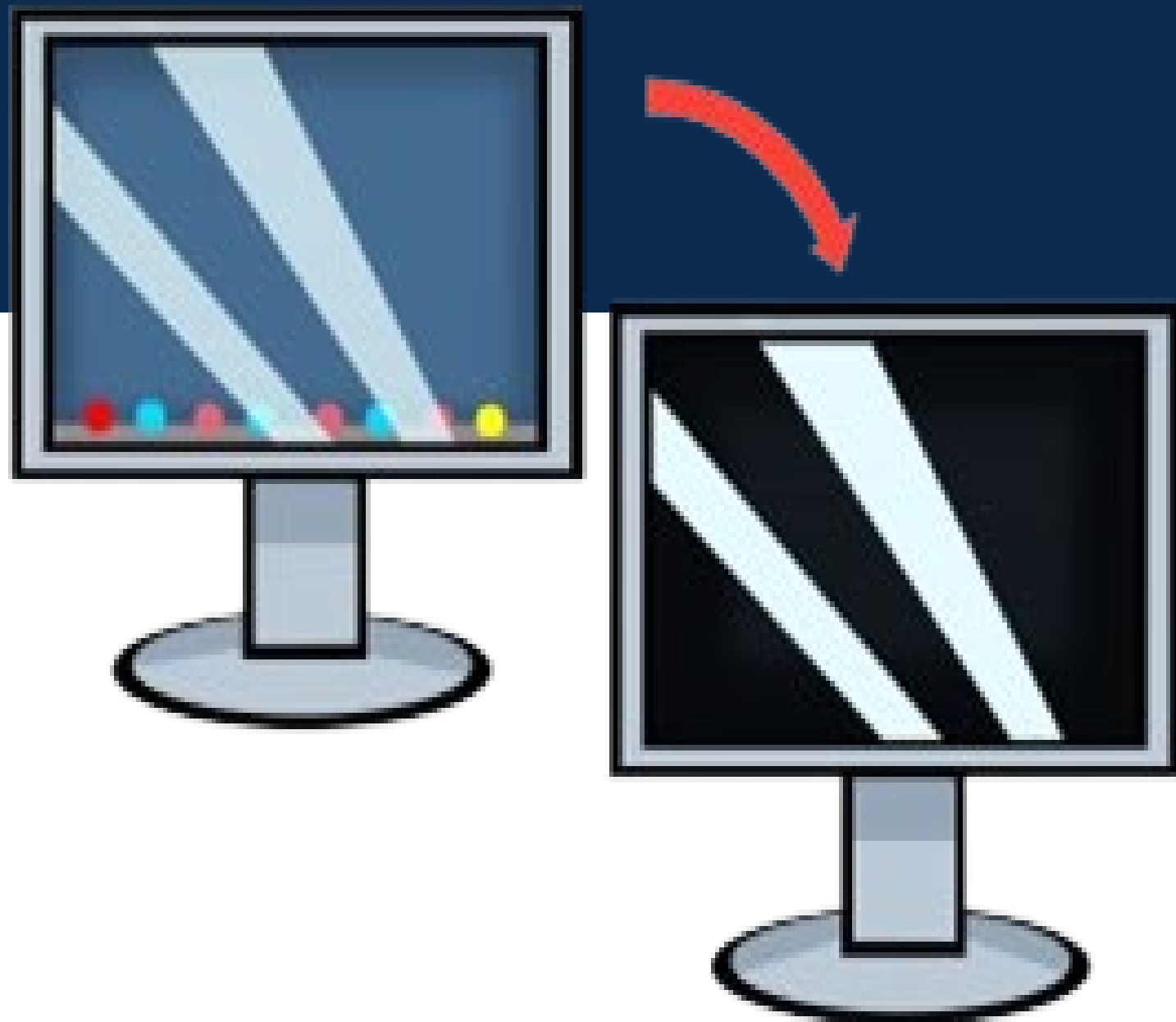


Physical Access

- Secure location
- Badge access only
- List of authorized personnel maintained by deputy director of BCI



**AUTHORIZED
PERSONNEL
ONLY**



Computer Sites

- Secure location
- Screen is not visible by unauthorized users
 - Monitors need to be facing away from windows viewable by the public
 - Monitors that cannot be moved away from windows need a privacy screen
- Log off UCJIS when not in use
- Lock your screen
- Keep all printouts from UCJIS in a secure area

Visitors

- Visitors must be accompanied at all times
- BCI keeps a visitor log. You can find these by both doors that come into the main BCI area



Information Security



Information Security

- All UCJIS files are subject to federal, state, and local laws and policies
 - CJIS Policy
 - UCA 53-10-108
 - Administrative Rule R722-900
 - Driver's Privacy Protection Act

Information Security

- UCA 53-10-108 (12)(a)
 - Class B misdemeanor for a person:

“...to knowingly or intentionally access, use, disclose, or disseminate a record created, maintained, or to which access is granted by BCI or any information contained in a record created, maintained, or to which access is granted by BCI for a purpose prohibited or not permitted by statute, rule, regulation, or policy of a governmental entity.”

Misuse



UCJIS

Utah Criminal Justice
Information System



Misuse

- Anything that doesn't fall under the scope of Administration of Criminal Justice or Criminal Justice Employment is misuse
 - Curiosity checks are never ok
- Misuse can lead to:
 - Civil lawsuits
 - Criminal prosecution -Misdemeanor B
 - Loss of access for user, agency and/or state



Monitoring Misuse

- Misuse is monitored by agency logs
 - Regularly or by request
- Audits
- BCI Supervisors monitor logs weekly for:
 - Famous names
 - Family names
 - Purpose codes
 - Vague or non-unique auditing purpose

Dissemination

- Dissemination is giving or sharing UCJIS information to another person
- Secondary dissemination is giving or sharing UCJIS information outside of your agency
 - This must be logged with a Secondary Dissemination Log
 - Who requested the file
 - What file was disseminated
 - When it was requested
 - Why it was requested

Dissemination

- Example:
 - BCI disseminates CH information with ROAs
 - Automatically logged by UCJIS, BCI doesn't keep a physical secondary dissemination log for these


Dissemination

- Is giving confirmation that someone does or doesn't have a criminal history dissemination?
 - Yes
- Is dissemination only in print form?
 - No
 - Verbal and electronic dissemination is included

Actual Misuse Cases

- City official pressured officers for a copy of his son's warrant arrest
 - Disciplined and written up by department
- Dispatcher live streamed during shift and caught UCJIS data another employee asked about
 - Terminated by department
- Officer ran 'curiosity' records checks on women he met at a party
 - Lost POST certification, terminated by department
- State employee ran neighbors' criminal history and shared information with spouse
 - Terminated by department, criminal and civil charges filed

Role Based Training



All individuals with
unescorted access to
a physically secure
location



General Users



Privileged Users



Organizational
Personnel with
Security
Responsibilities

Who

- BCI term
 - Users and Non-access Users
- Those who login directly to access UCJIS and those who don't login, but request and receive UCJIS information

Minimum Required Training

- Everything in the previous role including:
 - Criminal Justice Information
 - Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information
 - Personally Identifiable Information
 - Information Handling
 - Media Storage
 - Media Access
 - Audit Monitoring, Analysis, and Reporting
 - Access Enforcement
 - Least Privilege
 - System Access Control
 - Access Control Criteria
 - System Use Notification
 - Session Lock
 - Personally Owned Information Systems
 - Password
 - Access Control for Display Medium
 - Encryption
 - Malicious Code Protection
 - Spam and Spyware Protection
 - Cellular Devices
 - Mobile Device Management
 - Wireless Device Risk Mitigations
 - Wireless Device Malicious Code Protection
 - Literacy Training and Awareness/Social Engineering and Mining
 - Identification and Authentication (Organizational Users)
 - Media Protection



Training Example

Information Security



Mobile Devices

- Mobile devices used to access UCJIS information must have:
 - Remote locking of device
 - Remote wiping of device
 - Setting and locking device configuration
 - Detection of “rooted” and “jailbroken” devices
 - Enforcement of folder or disk level encryption
 - Application of mandatory policy settings on the device
 - Detection of unauthorized configurations
 - Detection of unauthorized software or applications
 - Ability to determine the location of agency-controlled devices
 - Prevention of unpatched devices from accessing CJI or CJI systems
 - Automatic device wiping after a specified number of failed access attempts

Mobile Devices

- BCI employees who have a mobile device for work purposes, these were installed prior to you receiving the device

Storage

- S drive
- Local drive
- Print
 - Store in a secure location
 - Do not leave CJIS information on desk or in an open area

Destruction

- Devices are wiped 3 times
- Printed information
 - Cross-cut shred
 - Burned
- CD/disks
 - Cut up
 - Shredded

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



Baiting

- Asking questions to probe for information



Piggybacking or Tailgating

- An authorized person lets an unauthorized person through a secure area intentionally or accidentally
- An unauthorized person following a authorized person into a secure area



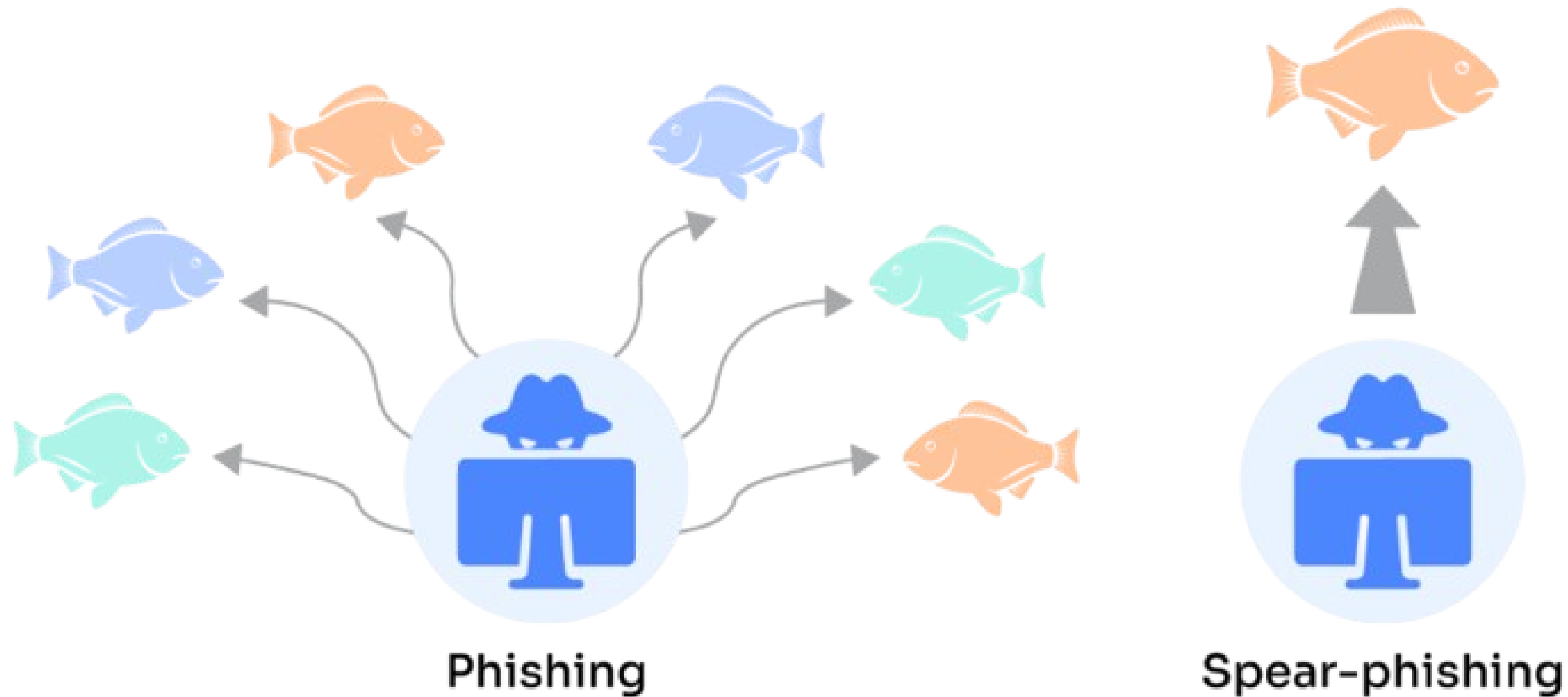
Shoulder Surfing

- Viewing what someone is working on on their computer screen
 - Can also be listening in on conversations



Phishing

- Phishing
 - E-mails asking for personal data
- Spear phishing
 - Targets a specific person
 - Appears to come from a trusted source



Social Mining


- Social mining is an attempt to gather information about the organization that may be used to support future attacks




User Security



UCJIS

- The User ID and Agency identifies you
- UCJIS will track every transaction under your User ID once you login
- If you step away from your station, please lock your screen with  + L

**If you are not
actively using UCJIS,
please logout**



UCJIS

Utah Criminal Justice
Information System


User Authentication


User

ybear

Agency

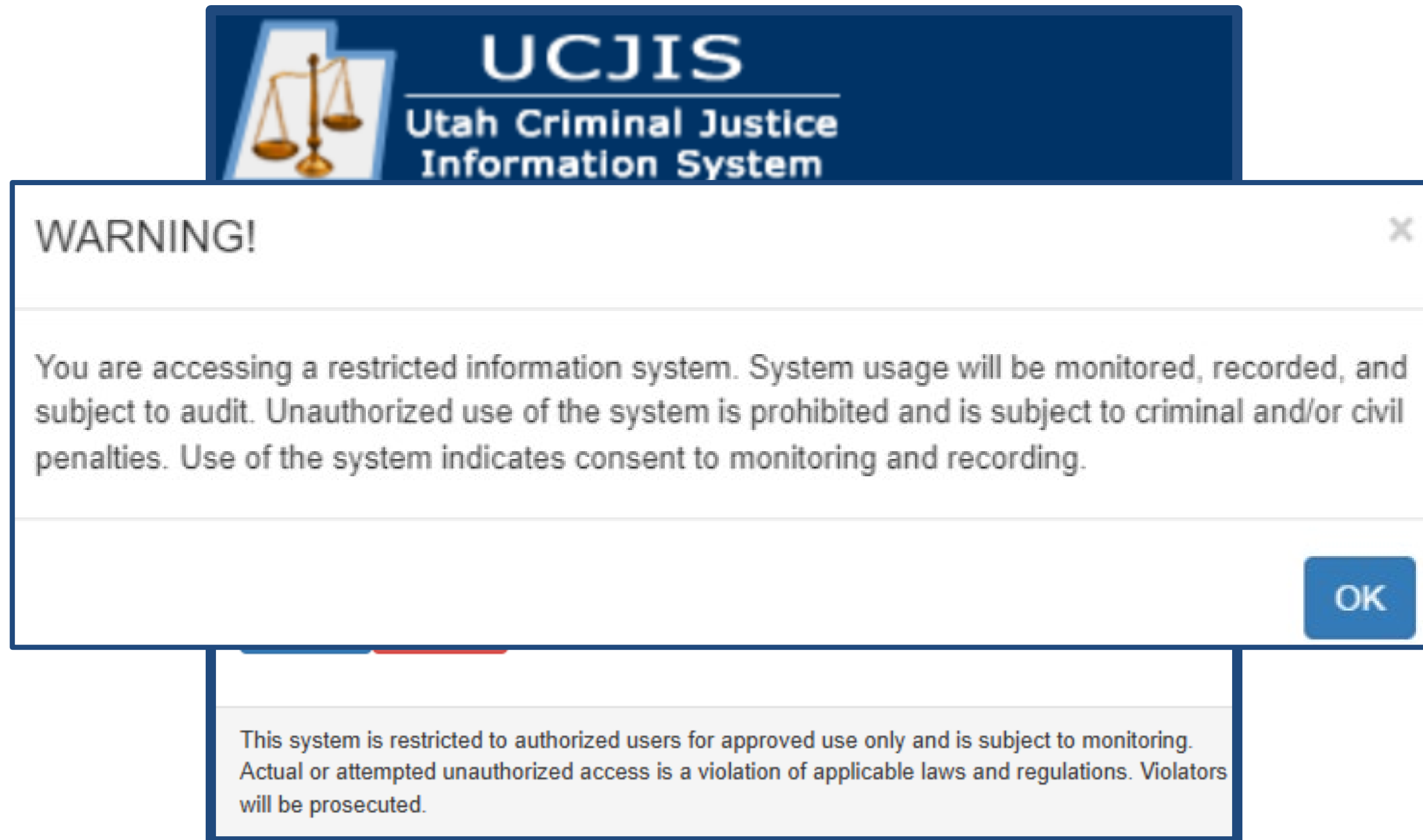
BCIFS

 Login

 Reset

This system is restricted to authorized users for approved use only and is subject to monitoring. Actual or attempted unauthorized access is a violation of applicable laws and regulations. Violators will be prosecuted.

UCJIS



User ID Responsibility



- Please remember:

**Anything that is ran
under your User ID is
your responsibility**



User Training & Testing Agreement

- Users must be trained and tested within 6 months of their hire date
- They also must be re-trained and re-tested every 2 years thereafter
- The agreement must be submitted at least every 2 years

UCJIS USER TRAINING AND TESTING AGREEMENT UCJIS NON-ACCESS USER TRAINING AGREEMENT	
for	
	
<div></div> USER OR NON-ACCESS USER (Please Print)	<div></div> USER OR NON-ACCESS USER ID
This agreement must be signed and submitted to BCI after the completion of the user or non-access user's initial training and testing <i>and</i> after each biennial training and testing.	
UTAH ADMINISTRATIVE RULE R722-900 DEFINITIONS:	
USER: a person working for or with an agency who has direct access to UCJIS.	
NON-ACCESS USER: a person working for or with an agency who asks for and/or receives UCJIS records.	
REQUIRED TRAINING OF EACH USER AND NON-ACCESS USER:	
RESTRICTIONS ON ACCESS, USE, AND CONTENT OF UCJIS RECORDS: UTAH CODE 53-10-108 <input type="checkbox"/>	
DISSEMINATION, PRIVACY, AND SECURITY OF UCJIS INFORMATION <input type="checkbox"/>	
CJIS REQUIRED SECURITY AWARENESS TRAINING <input type="checkbox"/>	
REQUIRED TRAINING AND TESTING FOR USER:	
BCI MANUALS AND/OR NCIC MANUALS: LOCATION AND USAGE <input type="checkbox"/>	
PLEASE CHECK THE FILES THE USER WAS TRAINED AND TESTED ON:	
DLD <input type="checkbox"/>	NLETS <input type="checkbox"/> MVD <input type="checkbox"/> III <input type="checkbox"/>
UCH <input type="checkbox"/>	NCIC Inquiry <input type="checkbox"/> NCIC Entry <input type="checkbox"/> SWW/PO <input type="checkbox"/>
UCJIS CERTIFICATION: The TAC has updated the CERT transaction: Yes <input type="checkbox"/> No <input type="checkbox"/>	
This certifies that this user or non-access user has passed all of the required training and proficiency testing to be able to access UCJIS information.	
UCJIS USER AND NON-ACCESS USER AGREEMENT	
I certify that by signing this document that I have been trained and/or proficiency tested according to the procedure set by my agency, BCI, and CJIS. I accept that I will be held accountable for any information accessed under my user ID. I understand per <u>Utah Code Annotated 53-10-108 (12)(a)</u> , it is a class B misdemeanor for a person to knowingly or intentionally access, use, disclose, or disseminate a record created, maintained, or to which access is granted by BCI or any information contained in a record created, maintained, or to which access is granted by BCI for a purpose prohibited or not permitted by statute, rule, regulation, or policy of a governmental entity.	
USER OR NON-ACCESS USER'S SIGNATURE	
<div></div>	
TAC SIGNATURE	DATE SIGNED BY TAC
<div></div>	<div></div>
AGENCY	ORI
Please submit to your BCI Field Services representative or bcifs@utah.gov per Utah Administrative Rule R722-900-4	
Revised May 2024	

Passwords

- Passwords are valid for 90 days and expire at midnight
- Password length will change on **1/1/2025**
 - Passwords will need to be longer than 8 characters (CJISSECPOL IA-5(1)(a)(5))
 - Do not use personal information
 - Avoid using anything similar to your Login ID
 - Cannot be identical to the previous 10 passwords
 - Include upper and lower case letters
 - Include special characters
 - !^*()_-=+;:.,{}[]

Passwords

- Please do not store your passwords anywhere accessible or viewable by the public or anyone else
- This includes, but is not limited to:
 - Writing it down on post it notes & leaving them around your computer
 - Pinning it to your corkboard
 - Storing it in your filing cabinet

Session Lock

- Other
 - 30 minutes
- Law Enforcement
 - 60 minutes

59:59 until timeout


Privacy & Security Training

<https://ucjis-tac.utah.gov/wp-content/uploads/sites/38/2023/10/Privacy-Security-Awareness.pdf>

Revised October 2023



Role Based Training



All individuals with
unescorted access to
a physically secure
location



General Users



Privileged Users



Organizational
Personnel with
Security
Responsibilities

Who


- BCI term
 - Non-users
- IT not LASO



Minimum Required Training

- Everything in the previous roles including:
 - Access Control
 - System and Communications Protection and Information Integrity
 - Patch Management
 - Data backup and storage—centralized or decentralized approach
 - Most recent changes to the CJIS Security Policy

Role Based Training



All individuals with
unescorted access to
a physically secure
location



General Users



Privileged Users



**Organizational
Personnel with
Security
Responsibilities**

Who

- BCI term
 - Non-access user
- LASO

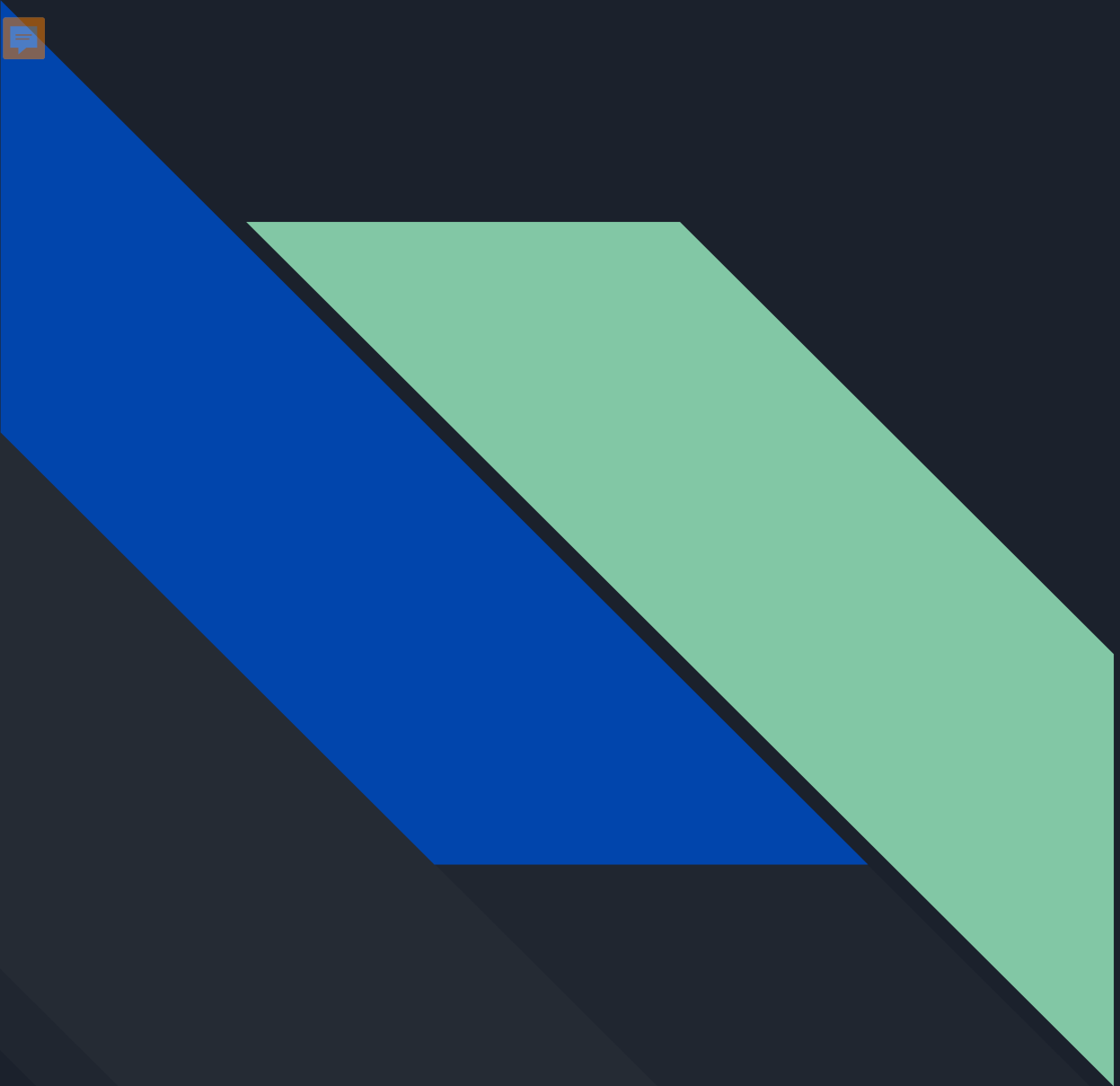


Minimum Required Training

- Everything in the previous roles including:
 - Local Agency Security Officer Role
 - Authorized Recipient Security Officer
 - Additional state/local/tribal/territorial or federal agency roles and responsibilities
 - Summary of audit findings from previous state audits of local agencies
 - Findings from the last FBI CJIS Division audit



Training Example



Enhanced Awareness Training for LASOs (2024)

<https://ucjis-tac.utah.gov/wp-content/uploads/sites/38/2023/01/2022-LASO-Training.pdf>

Utah Department of Public Safety

Introductions

Tyson Jarrett
Utah CJIS ISO



TJarrett@utah.gov
(385) 255-0888


Jarrel Beal
Utah CJIS SME



JarrelBeal@utah.gov
(385) 253-2420



Contacts

- Audit and general CJIS questions
 - CJISITS@utah.gov 
- Jarrel Beal - CJIS SME
 - JarrelBeal@utah.gov (385-253-2420)
- Tyson Jarrett - CJIS ISO
 - TJarrett@utah.gov (385-255-0888)
- FBI CJIS ISO Team
 - iso@fbi.gov

Tracking Training



CJIS Policy AT- 4

Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training and retain individual training records for a minimum of three years



How?

- Use SAT

Security Awareness Training

Enter Security Awareness Training Date

[Click here to see more information on how to use this transaction.](#)

User Details

User ID: *

ENTER USER ID

Agency: *

BCIFS

Training Date: *

ENTER TRAINING DATE MMDDYYYY

Test Date must be within the past 30 days.

By entering a Train/Test Date, I acknowledge that I have trained the individual on all Security Awareness requirements.

How?

- Create a spreadsheet

Security Awareness Training Date Tracker					
Name	User ID	Initial Training Date	Most Recent Training Date	Next Training Due	Role
Bear, Yogi	ybear	6/5/2024	6/5/2025	6/5/2026	General User
Hopps, Judy	jhopps	6/5/2024	6/5/2025	6/5/2026	General User
George, Regina	zzgeorge	3/3/2024	3/3/2025	3/3/2026	Privileged User
Gilmore, Lorelai	zzlorela	3/1/2024	3/3/2025	3/3/2026	All individuals with unescorted access to a physically secure location
Howard, Barbara	bhoward	8/4/2024		8/4/2025	Organizational Personnel with Security Responsibilities
Day, Jessica	jday	12/1/2024		12/1/2025	General User

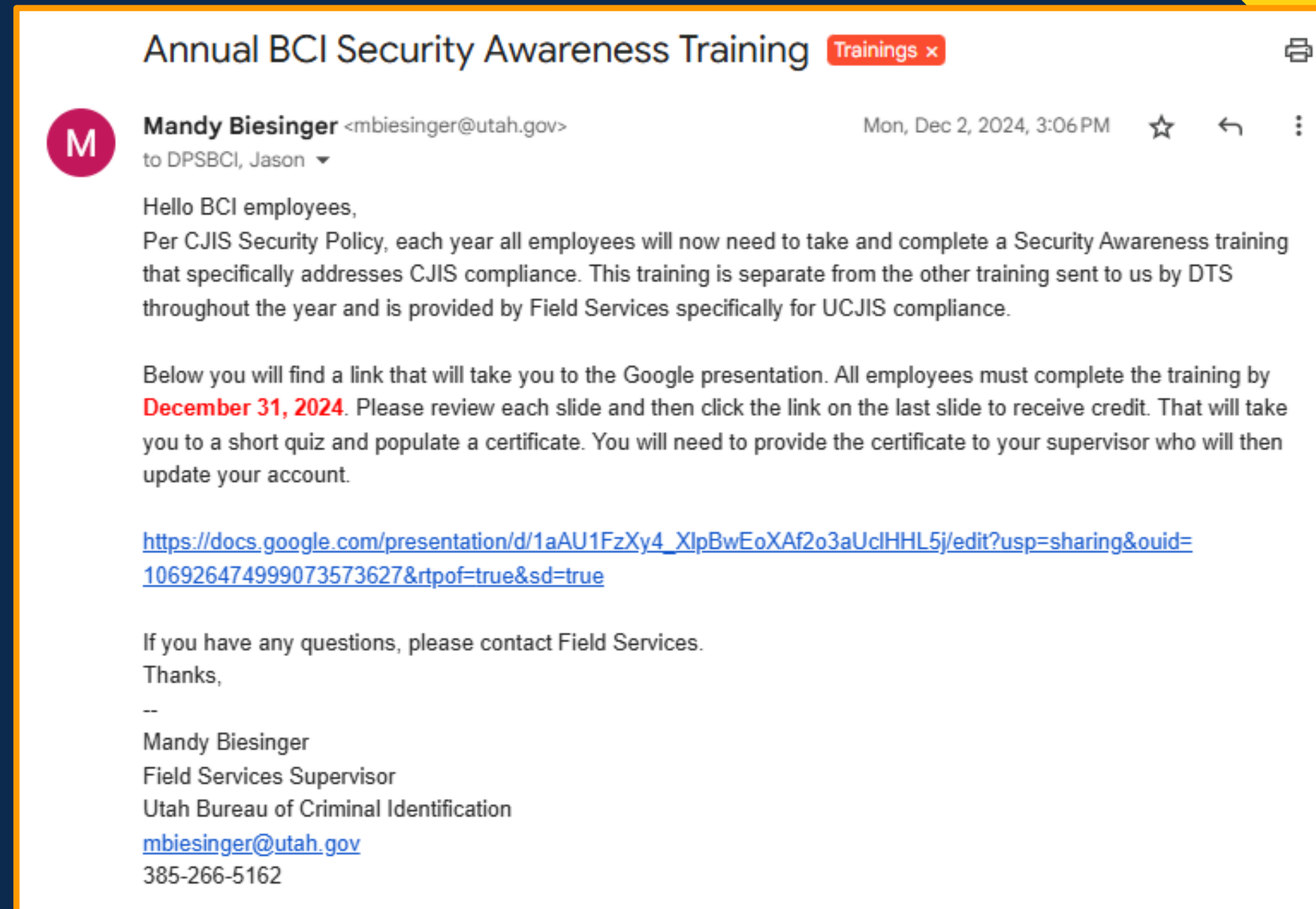
How?

- Create a spreadsheet

Security Awareness Training Date Tracker			
Name	User ID	Next Training Due	Role
Bear, Yogi	ybear	6/5/2026	General User
Hopps, Judy	jhopps	6/5/2026	General User
George, Regina	zzgeorge	3/3/2026	Privileged User
Gilmore, Lorelai	zzlorela	3/3/2026	All individuals with unescorted access to a physically secure location
Howard, Barbara	bhoward	8/4/2025	Organizational Personnel with Security Responsibilities
Day, Jessica	jday	12/1/2025	General User

How?

- Email agency with training materials



How?

- Email agency with training materials



BCI Security Awareness Training

BCI Security Awareness Training 2024

Please answer the following questions and acknowledge that you have completed the training.

ovaisima@utah.gov [Switch account](#)

Not shared

* Indicates required question

Email *

Your answer

Full Name *

Your answer

BCI Section *

Your answer

Please check all that are social engineering techniques *

0 points

- ☐ Baiting
- ☐ Piggybacking
- ☐ Social mining
- ☐ Shoulder surfing
- ☐ Phishing
- ☐ These are all social engineering techniques

Due to CJIS Policy changing, security awareness training will now be held *

0 points

- ☐ Biennially
- ☐ Annually
- ☐ Only when an incident occurs
- ☐ Only when policy updates
- ☐ Annually AND if an incident occurs (with involved individuals), if there are system changes, or if policy changes

Where are the visitor logs located at BCI? *

0 points

- ☐ Both doors that come into the main BCI area
- ☐ By the mailroom
- ☐ By the printers

I acknowledge that I have completed the BCI Security Awareness training *

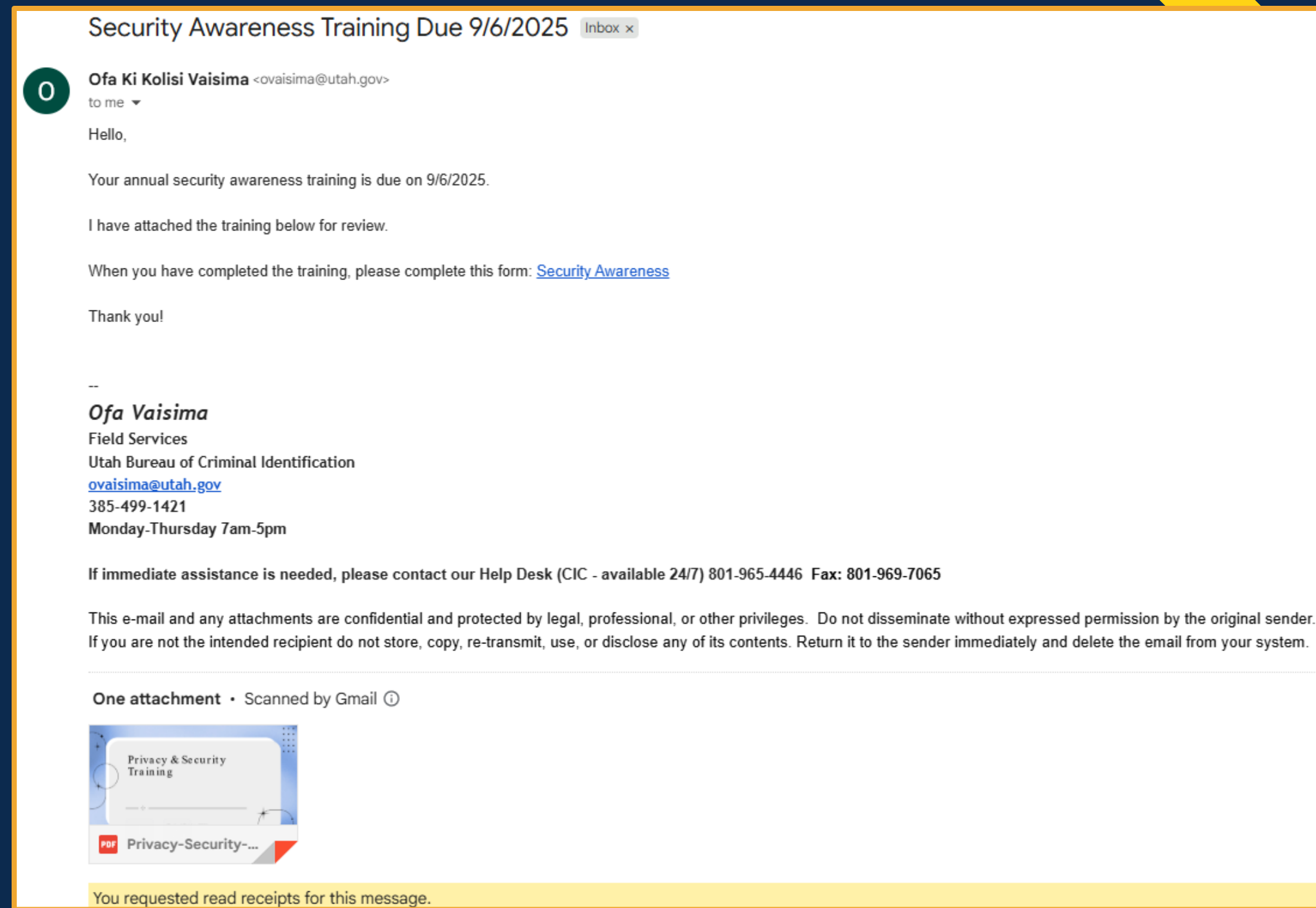
(Please enter the date you completed training)

Date

mm/dd/yyyy

How?

- Email and turn on read receipts

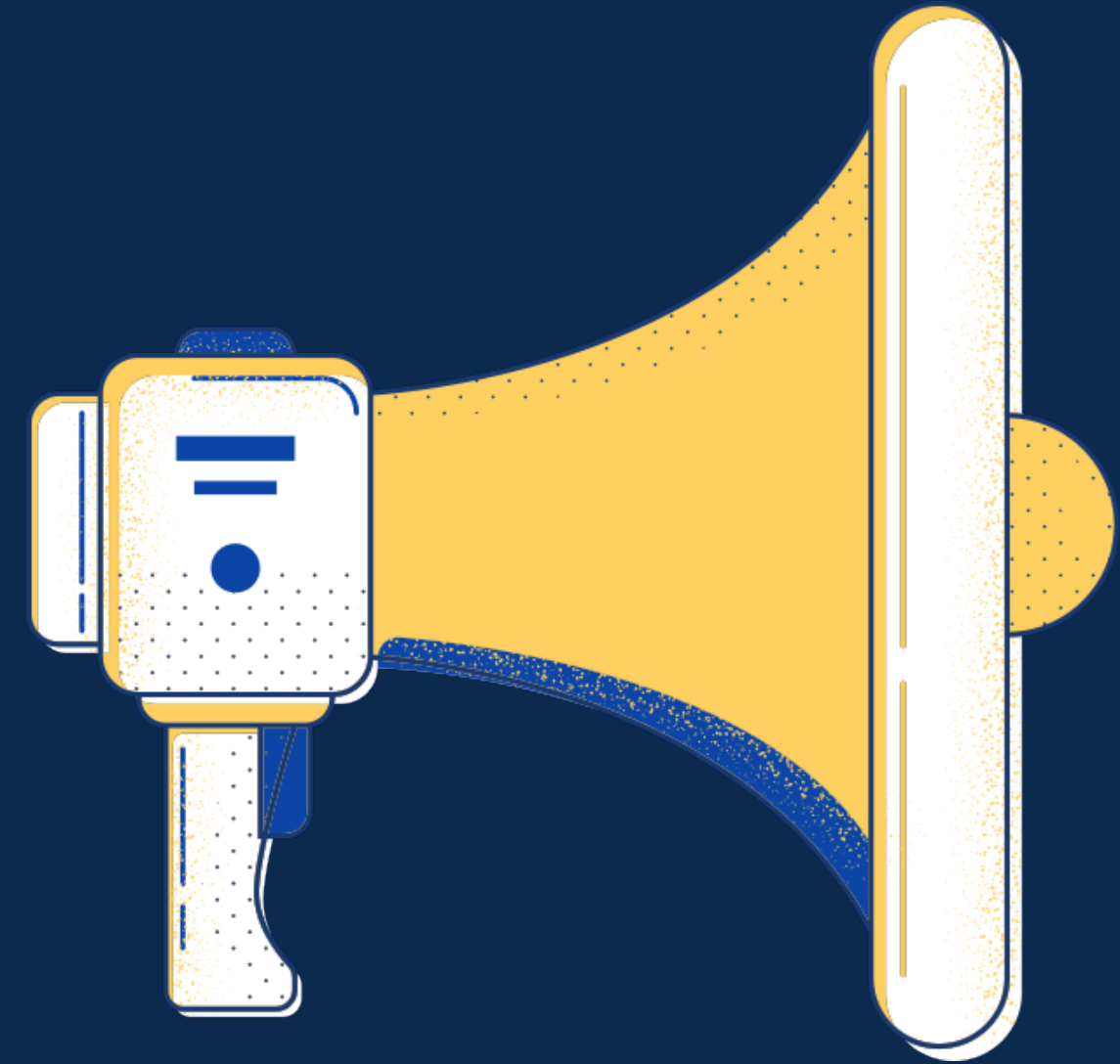


Training Ideas



Agency Wide Training

- Host a group review all at once
 - Time scheduled out to focus on Security Awareness
 - Month full of Security Awareness events
 - One meeting designated to SAT
 - Week of Security Awareness events



Examples



Examples

CJIS Security Awareness Training

JYUDBILSHZUATRVPHV RVZKLBAYLURR
RCIQYCEGVWIMOELCWZMBIBNOPWCNK
YTFYESHHCYUEMBMAHDMDEPXSXODOISX
YUNDKILTTTRVUGCLUJQBZIDFWXLKIOT
YUJCYBXGYYZDEDEYUENHWGCSAEKZNC
VTNYKAGUCKYVLZUBFMHIGTIJSGTDIM
WEGUENCNVGCIBPAJUFMWYAKTVYNKAL
JEXXWLTKRUGSSYARRLOKBURBPYIALW
NMYFVESLHQCIMWUSOVR SADCHZSHCEB
EGJTBHCJZZATMKUKPZSNCRBIVBSFNL
FDVHMZTGLMPOMMVMHAFOKVUZBJSEGS
ELPKWRSHLXJRLYKZMHTXIXZPLCIVIK
WANXFIOMYTJCOCBMEKURNIT IPEVUNR
DCMDYQLAHMKOCPCYXAYQGTFAQITVES
WRTRVZWFAQATNHDHLIHUQBYLFMONCEI
YARGIVRMYBFTQTBYS CGGZFOEISHERT
DFGKHYWZIPJ RMAOVWJDQQIKXSXS SIN
IYLMKXQWOFPOWSUZKIKDSVYAUBKDNP
VCBVDXWXOCALGENERALUSERMSXUSGV
DISSEMINATIONLEXGIWPNKNREUBFVB
IAAAUTBSTREJNETUMVKVHQC PNMWGUT
QAPJKRFL LGURZMCGYHACLWTFUBLYFW
IVYE PNSJEBXEPDQ RDMBVUZAKHNHYU
KCECGMROCYFBLUJEVKYLQUVOFDMIGX
ZBRYREXJMEXKADGTOSFUTXHHGCPDDO
AVOARBVCENZISVYEDRDPAFGLTDTSLT
VFOVXXPGMONAOQDWGUWNRWLVLFULWL
KIPRPAFDYKZRCRTCADZOGJLQVTOMLF
NZFTPMVCWOHSI IHBGEPUQWYAEYQXTW
OHXAHZZMVICJOLBAITINGCPWNHNTFD

The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes

An authorized person lets an unauthorized person through a secure area intentionally or accidentally

knowingly or intentionally access, use, disclose, or disseminate a record created, maintained, or to which access is granted by the division or any information contained in a record created, maintained, or to which access is granted

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 escort visitors at all times and monitor visitor activity.

A user, but not a process, who is authorized to use an information system

The primary Information Security contact between a local law enforcement agency and the CSA under which this agency interfaces with the FBI CJIS Division.

Sharing CJIS information with authorized users

Asking questions to probe for information

Use definitions instead of the word

The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes

An authorized person lets an unauthorized person through a secure area intentionally or accidentally

knowingly or intentionally access, use, disclose, or disseminate a record created, maintained, or to which access is granted by the division or any information contained in a record created, maintained, or to which access is granted

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 escort visitors at all times and monitor visitor activity.

A user, but not a process, who is authorized to use an information system

The primary Information Security contact between a local law enforcement agency and the CSA under which this agency interfaces with the FBI CJIS Division.

Sharing CJIS information with authorized users

Asking questions to probe for information

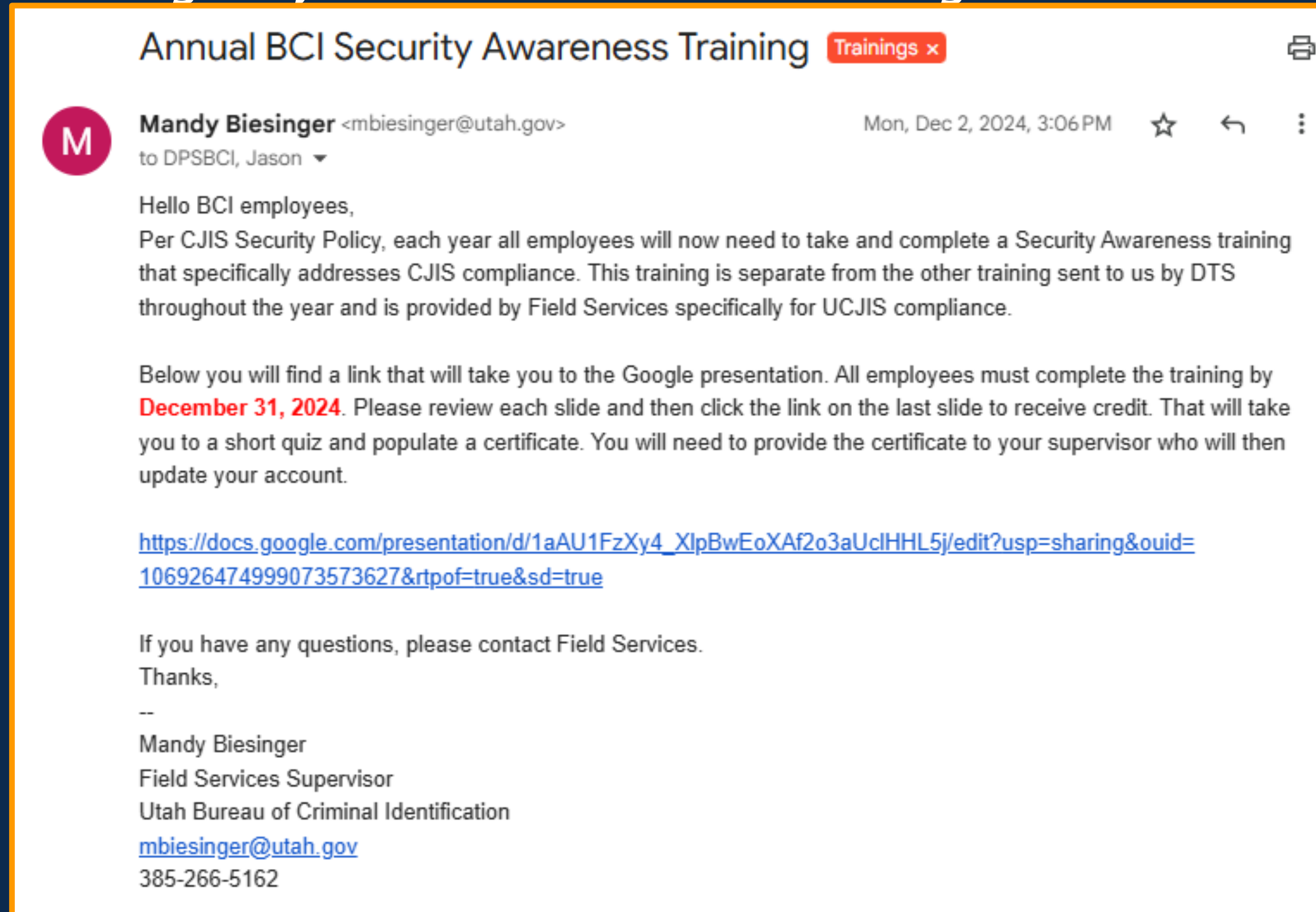
Self Review

- Provide your agency with an SAT presentation via Email for self review
- Provide a way to ensure that the presentation was reviewed
 - Google Form
 - Survey Monkey
 - Read receipts, etc.



Example

- BCI sends out an agency wide email with training materials



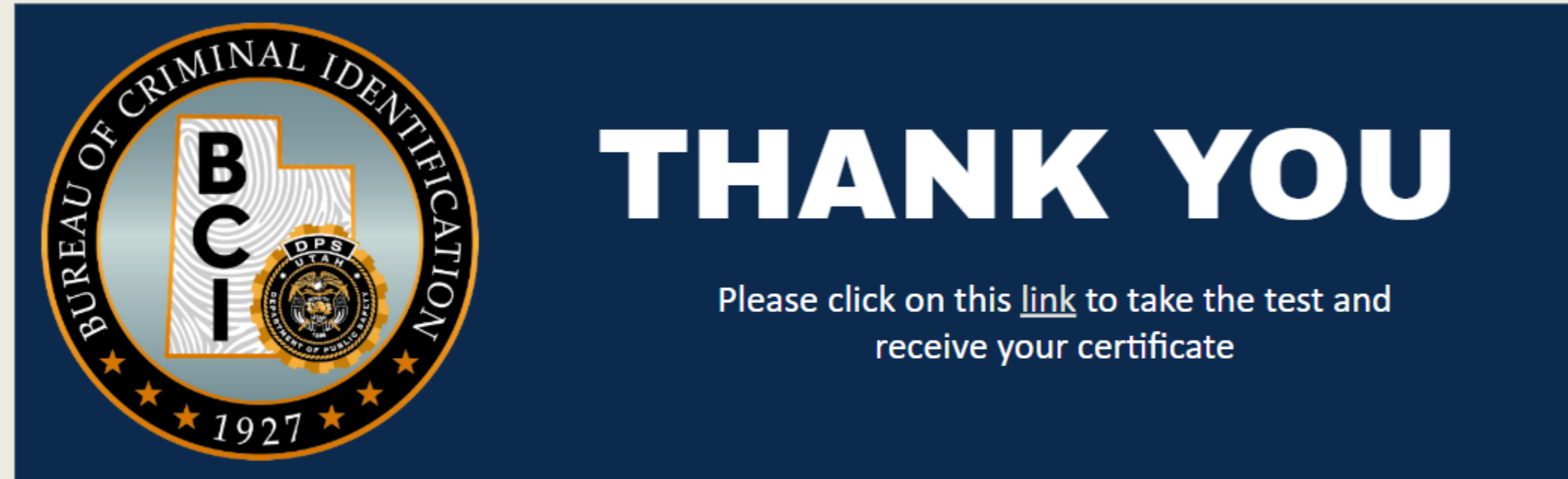
Example

- Training materials include a presentation for employees to review





Example

- At the end of the presentation, BCI provides a link to a short quiz



Example



BCI Security Awareness Training

Please answer the following questions and acknowledge that you have completed the training.

ovaisima@utah.gov [Switch account](#)

Not shared

* Indicates required question

Email *

Your answer

Full Name *

Your answer

BCI Section *

Your answer

Who would be held responsible between Chief Wiggum and Homer for misusing the system? * 1 point

☐ Chief Wiggum

☐ Homer

Do you have a better understanding of Misuse and Dissemination? * 1 point

☐ Yes

☐ No

I acknowledge that I have completed the BCI Security Awareness training * 1 point

☐ Yes

Submit

Clear form

Never submit passwords through Google Forms.

This form was created inside of State of Utah. - [Contact form owner](#)

Example

- Automatically generates a tracker when the form is completed

A	B	C	D	E	F	G	H
Timestamp	Score	Email	Full Name	BCI Section	Who would be held responsible	Do you have a better understanding of the process?	I acknowledge that I have read and understood the information provided
3/30/2020 16:16:52	3 / 3	t		CIC	Chief Wiggum	Yes	Yes
3/30/2020 16:19:14	3 / 3	c		Field Services	Chief Wiggum	Yes	Yes
3/30/2020 16:20:31	3 / 3	r		Field Services	Chief Wiggum	Yes	Yes
3/30/2020 16:22:35	3 / 3	e		Support Services	Chief Wiggum	Yes	Yes
3/30/2020 16:34:06	3 / 3	e		AFIS	Chief Wiggum	Yes	Yes
3/30/2020 16:52:22	3 / 3	e		Grants	Chief Wiggum	Yes	Yes
3/30/2020 17:49:12	3 / 3	t		AFIS	Chief Wiggum	Yes	Yes
3/30/2020 20:47:22	3 / 3	r		Records	Chief Wiggum	Yes	Yes
3/30/2020 22:35:35	3 / 3	r		Records	Chief Wiggum	Yes	Yes
3/31/2020 5:39:27	3 / 3	h		AFIS	Chief Wiggum	Yes	Yes
3/31/2020 5:40:43	3 / 3	j		AFIS	Chief Wiggum	Yes	Yes
3/31/2020 7:20:45	3 / 3	a		Field Services	Chief Wiggum	Yes	Yes
3/31/2020 7:30:26	3 / 3	g		Field Services	Chief Wiggum	Yes	Yes
3/31/2020 7:31:47	3 / 3	l		Firearms	Chief Wiggum	Yes	Yes
3/31/2020 7:39:05	3 / 3	r		Expungements	Chief Wiggum	Yes	Yes
3/31/2020 8:13:36	3 / 3	c		AFIS	Chief Wiggum	Yes	Yes
3/31/2020 8:21:26	3 / 3	c		Grants	Chief Wiggum	Yes	Yes

Example

- TAC can use responses to create separate tabs with the sections or departments in your agency. This will allow you to provide a list to that section/department supervisor of users and non-users that still need to take the training

ABC ▾ CIC ▾ Admin ▾ AFIS ▾ Brady ▾ Expungements ▾ Field Services ▾ Firearms ▾ Grants ▾ Records ▾ Support Services ▾

Example

- Generate a certificate that the user or non-user will need to send to the TAC when they complete the training



Staff Meetings

- Cover SAT over time
 - Staff meetings are already required
 - Cover a specific item each meeting
 - Can be quick



Example

- Shoulder surfing in regards to CJIS data and conversations including CJIS information



- Sending secure emails with CJS information

New Secure Message

Virtru Protection ON ⓘ

⚙️

🔒

ToCc Bcc 👤 +

SubjectPersonal Introduction ▾

--

Ofa Vaisima
Field Services
Utah Bureau of Criminal Identification
[ovaisima@utah.gov](#)
385-499-1421
Monday-Thursday 7am-5pm

If immediate assistance is needed, please contact our Help Desk (CIC - available 24/7) 801-965-4446 Fax: 801-969-7065

This e-mail and any attachments are confidential and protected by legal, professional, or other privileges. Do not disseminate without expressed permission by the original sender.
If you are not the intended recipient do not store, copy, re-transmit, use, or disclose any of its contents. Return it to the sender immediately and delete the email from your system.

↶ ↷ Sans Serif ▼ ⌨ ▼ **B** *I* U A ▼ ☰ ▼ ≡ ≡ ≡ ≡ ▾

Secure Send ▾

A ✎ 📎 🔗 😊 🖼️ 🪄 📅 ⋮ 🗑️

Agency Newsletter

- Send out a newsletter with SAT



Example

UTAH BCI NEWSLETTER

ISSUE 25.3 AUGUST 2025



Utah Bureau
of Criminal
Identification
Newsletter

Information Security

Reminder: Access to UCJIS information should be only for the following reasons:

- Administration of CJ
 - Detection
 - Apprehension
 - Detention
 - Pretrial release
 - Post-trial release
 - Prosecution
 - Adjudication
 - Correctional supervision
 - Rehabilitation of accused persons or criminal offenders
- CJ Employment

If you are around UCJIS information when in a secure area, whether you are directly accessing it or it is in a visible location (on a coworker's desk), ensure you are following proper protocols. Do not disseminate information to unauthorized individuals, do not take UCJIS information from other's workspaces, etc.

UCA 53-10-108(12)(a)

"...to knowingly or intentionally access, use, disclose, or disseminate a record created, maintained, or to which access is granted by BCI or any information contained in a record created, maintained, or to which access is granted by BCI for a purpose prohibited or not permitted by statute, rule, regulation, or policy of a governmental entity."

Passwords

Passwords must be longer than 8 characters (CJISSECPOL IA-5(1)(a)(5))

- Do not use personal information
- Avoid using anything like your Login ID
- Cannot be identical to the previous 10 passwords
- Include upper- and lower-case letters
- Include special characters
 - !^*()_-=+;,:'.{}[]

Social Engineering Techniques

This quarter's spotlight social engineering technique spotlight is **baiting**

Baiting occurs when you are being asked questions to probe for more information

Baiting in regards to UCJIS data would occur if you are helping an individual face to face or over the phone and they want more information than we can legally give. Be aware of the questions you are being asked and answer them with caution. Please note, confirming criminal history status is a form of dissemination and would be considered misuse.

Updating Training Materials



Training Materials

- Per CJIS Security Policy AT-2(c & d)
 - Update literacy training and awareness content annually and following changes in the information system operating environment, when security incidents occur, or when changes are made in the CJIS Security Policy; and
 - Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques

Training Materials



Keep a revision date on training materials

Training Materials



Have an overview slide where you can view easily what section of the presentation you have updates for

Training Materials

- Use incidents from your agency or another agency
 - Example: An employee from Zootopia PD opened a phishing email that led to a system wide hack of their agency and all users were unable to login
 - Show examples of a phishing email

Training Materials

- Use incidents from your agency or another agency
 - Example: An employee from Zootopia PD opened a phishing email that led to a system wide hack of their agency and all users were unable to login
 - Show examples of a phishing email
 - Example: User left CJI unattended and an unauthorized user took pictures of the CJI and shared it on social media

Training Materials

- Use incidents from your agency or another agency
 - Example: An employee from Zootopia PD opened a phishing email that led to a system wide hack of their agency and all users were unable to login
 - Show examples of a phishing email
 - Example: User left CJI unattended and an unauthorized user took pictures of the CJI and shared it on social media
 - Example: An administrator left their master key out on accident. The key was obtained by unauthorized personnel and they were able to access areas with CJI that they were not supposed to

Training Materials

- If you want or need examples
 - Talk to other TACs in your area
 - Reach out to your FS rep

THANK YOU

