Welcome!

Slide Notes

Welcome to the North Carolina Department of Revenue 2020 Information Security and Privacy Awareness Training.

This training is a review and reminder of how important it is for us as an agency to protect the taxpayer information entrusted to us by the people of North Carolina.
Learning Outcomes

At the conclusion of this training module, you will be able to:

- Explain the importance of Information Security and Privacy
- List the Data Classifications at Revenue
- Define Federal Taxpayer Information (FTI) and Federal Regulations
- Describe how Federal Taxpayer Information is used at Revenue
- Identify types of Confidential Data
- Explain State Law relating to taxpayer information
- Discuss Facility Security Reminders

Slide Notes

At the conclusion of this training module, you will be able to:

- Explain the importance of Information Security and Privacy
- List the Data Classifications at Revenue
- Define Federal Taxpayer Information (FTI) and Federal Regulations
- Describe how Federal Taxpayer Information is used at Revenue
- Identify types of Confidential Data
- Explain State Law relating to taxpayer information
Learning Outcomes, cont.

Learning Outcomes
At the conclusion of this training module, you will be able to:

- Explain the importance of Information Security and Privacy
- List the Data Classifications at Revenue
- Define Federal Taxpayer Information (FTI) and Federal Regulations
- Describe how Federal Taxpayer Information is used at Revenue
- Identify types of Confidential Data
- Explain State Law relating to taxpayer information
- Describe Staff Security Responsibilities
- Explain Email Best Practices
- Discuss Facility Security Reminders

Slide Notes, cont.

- Describe Staff Security Responsibilities
- Explain Email Best Practices
- Discuss Facility Security Reminders
Data Classifications

There are four data classifications used at Revenue. They are:

- Federal Taxpayer Information
- Confidential Information
- Public Information
- All Possible

We will discuss each of these within this training module, including the different types of confidential information that you may encounter while working at DOR.

Federal Taxpayer Information and Confidential Information should be protected and handled with care.
FTI and Federal Regulations

Slide Notes

The following section discusses Federal Taxpayer Information and Federal Regulations that are required at Revenue.
FTI and Federal Regulations, cont.

What is Federal Taxpayer Information or FTI?

Federal Taxpayer information is taxpayer information that is received directly from the IRS, and it may include the following:

- Any information that would identify a taxpayer. This may include their name, social security number, or their address.
- The nature, source, or amount of their income or salary.
- Payments or receipts.
- Deductions or exemptions on a tax return.
- Assets, liabilities, or net worth of a taxpayer.
A Federal Tax Return includes the following:

- Original or amended tax returns
- Tax Schedules
- Attachments
- Supplements for the tax return
FTI and Federal Regulations, cont.

Slide Notes, cont.

FTI can also include *business tax schedules* such as:

- Corporate (including S Corp)
- Partnership
- Withholding
- Excise

It’s important to note that the DOR receives information for audit results on these schedules.
FTI and Federal Regulations, cont.

Slide Notes

Working together, the Internal Revenue Service and Revenue share information regarding North Carolina taxpayers.

Revenue uses this information to:

- Update our income tax master files, including taxpayer names, addresses, and dates of death.
- Identify any persons or companies who did not file, and to identify taxpayers who underreport their income.
- Identify taxpayers who underreport their income.

All of this helps our agency recover lost revenue due to our State.
FTI and Federal Regulations, cont.

Federal Taxpayer Information and Federal Regulations

Slide Notes, cont.

Within the Internal Revenue Code section 6103, it states that Federal Tax Information may be disclosed to:

- The actual taxpayer of the tax return and return information.
- The taxpayer’s designee provided a Power of Attorney has been provided for this person from the taxpayer.
- State Tax Officials including Revenue staff with a business need to use information for tax administration purposes.
- Other persons who are authorized and with a need to know.

If you have questions regarding who you are able to disclose tax information to, please contact your supervisor.
Did You Know?

Federal Tax Information is still considered FTI regardless of whether it is in its original format.

If you copy Federal Tax Information, the copy is still considered Federal Tax information even if it is copied from one format to another (i.e., from electronic to hard copy, or from one type of word processor format to another).

Slide Notes

Did you know, if you copy federal tax information at all, even from one format to another, it is still considered federal tax information?

For example, if a NCDOR staff member generates a report that contains FTI through the use of an application on his/her workstation and then prints out the report, the printed report is also classified as FTI. All copies have the same handling requirements as the original document.

Remembering this concept will ensure that all FTI is tracked and logged accordingly per IRS requirement.
Slide Notes

During an average fiscal year, Revenue generates millions of dollars in increased collections based on information received from the Internal Revenue Service. So, you can see how valuable this information is to our agency.

Since most of the income surplus our agency has goes back to the state legislature, who in turn distributes it to other state agencies via budget allocations, it helps the entire state.

In order to keep receiving information from the Internal Revenue Service, we are required to adhere to federal laws and regulations. These include the Internal Revenue Service Publication 1075, and the Internal Revenue Code sections that are covered later in this training.
What is Commingling?

Commingled data is federal taxpayer information combined with state tax information.

Slide Notes

When FTI is combined with State tax information, it is referred to as Commingled data.

Commingling of Federal and State tax information subjects the entire file to the safeguard requirements mandated by the IRS.

Commingled data must be protected as required by the federal law from unauthorized access, disclosure, and inspection.
FTI and Federal Regulations

Federal Taxpayer Information and Federal Regulations

Never access or attempt to access taxpayer information for any of the following reasons:

Curiosity
Looking up celebrities or your neighbor's tax information.

Personal Use
Looking up an address. Never look up or attempt to modify your own account, family members, friends, acquaintances, or co-workers, etc.

Prior Work Assignments
Looking up a prior case no longer assigned to you without a business need.

Slide Notes

To protect FTI or commingled data, you should never access or attempt to access taxpayer information for any of the following reasons:

- **To satisfy a curiosity such as looking up celebrities or your neighbor’s tax information.**

- **For personal use such as looking up a taxpayer’s address.** You should never look up or attempt to modify account information for yourself, a family member, friends, acquaintances, co-workers, or anyone else without a business need.

- **To check on prior work assignments.** By looking up a prior case that is no longer assigned to you is considered accessing it without a business need.
FTI and Federal Regulations, cont.

If you are assigned an audit or you receive tax information for someone that you have a personal relationship with or know on a personal level as part of your job assignments, you should notify your supervisor immediately. Remember, all systems at Revenue are monitored. Unauthorized access and/or disclosure of taxpayer information is against Federal and State law.
Confidential Data

Now that we have defined Federal Taxpayer Information and Federal Regulations let’s identify the different types of confidential data that we must protect. Confidential data requires protection and proper destruction. It is important to understand what types of data are considered as confidential.

Confidential data includes:

1. Personal Identifiable information also referred to as Personally Identifiable Information.
2. Merchant Credit Card Data.
3. State Taxpayer Information.
Confidential Data, cont.

Other types of confidential data include but are not limited to:

5. Information System Security Data which includes data such as security configuration settings and other data about the security of our systems.


7. Contract Bids and Contract Bid Proposals that include identified vendor trade secrets.

8. Information provided by other state agencies for tax administration purposes.
State Laws and Taxpayer Information

Slide Notes

The next section in this training discusses State Laws and Taxpayer Information.
What are Public Records?

Public Records may include documents, paper, email, and text messages (defined in NC G.S. 132-1).

Public Records do not include confidential or protected communications (defined in NC G.S. 105-259).

Slide Notes

Public records may include documents, paper, email, text messages, or other means used to transact state business by any agency of North Carolina government, and are the property of the people as defined in NC G.S. 132-1.

Although these records are considered public property, there are limitations. Public records do not include confidential or protected communications as defined in NC G.S. 105-259.
Tax Information

NC G.S. 105-259. Secrecy required of officials; penalty of violation.

NC G.S. Chapter 132 defines public records.

If you receive a request for public records, please forward it to our Director of Public Affairs.

Slide Notes

The North Carolina General Statute 105-259 also states that we may not disclose tax information to any other person unless the disclosure is specifically permitted by the statute.

NC G.S. Chapter 132 defines public records. Therefore, if you receive a request for public records, please forward it to our Director of Public Affairs.
Protected Taxpayer Information

Taxpayer information is protected under the North Carolina General Statute 105-259.

Protected tax information includes the following:

- Information on a tax return, report, or an application for a license for which a tax is imposed.
- Information from an audit of a taxpayer, or correspondence with a taxpayer.
- Information about whether a taxpayer has filed a tax return or report.

The North Carolina General Statute applies to current and former staff and officers, as well as to contractors.
Slide Notes

In the event of an unauthorized disclosure of State Tax Information in regards to the North Carolina General Statute 105-259, the following penalties may apply under North Carolina State Laws:

- Class 1 Misdemeanor
- Dismissal from Public Office
- Termination of Employment without the possibility of rehire for five years
Destruction of Tax Information

Slide Notes

Should the agency no longer need certain tax information, there are procedures and processes in place that govern the disposal.

Paper must be shredded using a cross-cut shredder. **NOTE:** Shred size particles must be 1mm by 5mm, or smaller.

If shredding deviates from the above specifications, FTI must be safeguarded until it reaches the stage where it is rendered unreadable through additional means, such as burning or pulping.

**NOTE:** Hand tearing, recycling, or burying information in a landfill are unacceptable forms of disposal.
Destruction of Tax Information, cont.

FTI furnished or stored in electronic format must be destroyed in the following manner:

- Electronic media (e.g. hard drives, tapes, CDs, and flash media) must be destroyed according to guidance in **Section 9.3.10.6, Media Sanitization (MP-6), and Section 9.4.7, Media Sanitization**.

- Electronic media containing FTI must not be made available for reuse by other offices or released for destruction without first being subjected to electromagnetic erasing. If reuse is not intended, the tape must be destroyed by burning or shredding in accordance with applicable standards (see Table 13, Media Sanitization Techniques).

- Destroy microfilms (microfilm, microfiche, or other reduced image photo negatives) by burning.

When in doubt about how to dispose of tax information, please contact the Chief Information Security Officer.
The next section in this training discusses some requirements of the Payment Card Industry which Revenue must adhere to.
In the event your job or role requires a business need for you to collect credit card data from a taxpayer, certain precautions must be used in regard to handling and protecting this data:

- DOR staff must never store the CVC or Card Verification Code.
- You should never request the card verification code from the taxpayer.
- You must never store the card verification code which is sometimes called the pin verification code. This is the 3 or 4 digit code found on the back of credit cards or on the front of cards like American Express.
- You should never write the card verification code on paper, even if you intend to destroy later.
Payment Card Industry (PCI), cont.

Slide Notes, cont.

The Payment Card Industry allows us to store the 16-digit Primary Account Number which is located on the front (or back) of the card, but it must be stored in an encrypted format. Revenue stores this number encrypted and this is handled by our IT Department.

If you need to dispose of the card information in printed format, remember that the cardholder data must be disposed of in a way so that it cannot be reconstructed.
Personal Identifiable Information (PII)

Slide Notes

Personal Identifiable Information (PII) is Information that includes:

- A person’s first name or their first initial plus last name in combination with various types of identification numbers.

Under the North Carolina PII laws, business' information is also protected. Because this type of data is classified as “Confidential,” it must be properly handled and protected accordingly.
Personal Identifiable Information, cont.

PII Laws

“Person” definition under NC PII laws as defined in NC G.S. 75-61(9):

- Any individual, partnership, corporation, trust, estate, cooperative, association, government, or governmental subdivision or agency, or other entity.

Slide Notes, cont.

PII laws define the word **person** as referring to an individual, partnership, corporation, trust, estate, cooperative, association, government, or governmental subdivision or agency, or other entity.

An example of PII could include an individual’s first and last name along with their social security number, or a business name and a tax identification number.
It is important that staff understand what types of information are considered to be PII. Below is a listing of what Personal Identifiable Information may include under the North Carolina General Statute 14-113.20:

- Social Security or employer taxpayer identification numbers
- Driver's license
- State identification card or passport numbers
- Checking account numbers
- Saving account numbers
- Credit card numbers
- Debit card numbers
- Personal Identification (PIN) Code as defined by G.S. 14-113.8(6)
- Electronic Identification numbers, electronic mail names, or addresses
- Internet account numbers or internet identification names
- Digital Signatures
- Any other numbers or information that can be used to access a person's financial resources
- Biometric data
- Fingerprints
- Passwords
- Parent's legal surname prior to marriage
Personal Identifiable Information, cont.

Personal Identifiable Information may include under the NC G.S. 14-113.20:

- Social Security or employer taxpayer identification numbers
- Driver’s license
- State identification card or passport numbers
- Checking account numbers
- Saving account numbers
- Credit card numbers
- Debit card numbers
- Personal Identification (PIN) Code as defined by G.S. 14-113.8(6)
- Electronic Identification numbers, electronic mail names, or addresses
- Internet account numbers or internet identification names
- Digital Signatures
- Any other numbers or information that can be used to access a person’s financial resources
- Biometric data
- Fingerprints
- Passwords
- Parent’s legal surname prior to marriage

Slide Notes, cont.

- Internet account numbers or internet identification names
- Digital Signatures
- Any other numbers or information that can be used to access a person’s financial resources
- Biometric data
- Fingerprints
- Passwords
- Parent’s legal surname prior to marriage
What is excluded from PII?

Slide Notes

Besides knowing what is included in Personal Identifiable Information, it is also important to know what it is not included.

- According to the North Carolina General Statute 75-61, information in a publicly available directory that an individual has voluntarily consented to have publicly disseminated is not considered Personal Identifiable Information. For example, their name, address and telephone number listed in a phone directory.

- Also, information made lawfully available to the general public from federal, state, or local government records. For example, their name and address which is legally required to be made publically available and is found on the local property tax web site.
All Possible

The last data classification we will look at is All Possible. Occasionally you may run across data that is classified as “All Possible.” This is the highest classification that we have here at DOR.

What this means is that all of the regulations and requirements that the Agency is expected to follow should be applied to this data.
Staff Security Responsibilities

Slide Notes

The next section in this training covers Insider Threats.
Staff Security Responsibilities

Slide Notes

The security of data, as well as the safety of agency staff members, is the responsibility of everyone.

Here are a few reminders:

- Staff members should always be aware and observe their surroundings, and they should report any security violations to the Service Desk.

- There is no expectation of privacy when using Revenue owned Resources.

- Protect, and do not share, your logon credentials.

- Do not change any security settings of Resources.
Staff Security Responsibilities, cont.

Slide Notes, cont.

- Staff members should not put any offensive, libelous, harassing, or discriminatory statements into electronic communications such as text messages or emails.

- Do not attempt to access data, resources, or media that is not appropriate for your duties or which you are not authorized.

- Immediately report to the Service Desk any discovered access to resources or data that is not appropriate for yourself or other staff members.

- Report any suspicious behavior that might indicate an insider threat to the Service Desk.
Insider Threats

An Insider Threat is a malicious threat to an organization that comes from people within the organization.

All suspected Insider Threats must be reported to the Service Desk.

Slide Notes

An Insider Threat is a malicious threat to an organization that comes from people within the organization.

It is important that all staff know how to recognize potential indicators of an insider threat:

Some behaviors that you may observe in the individual are as follows:

- Violating agency policy
- Showing disregard for rules
- Working odd hours without authorization
Insider Threats, cont.

• Unnecessary copying of material, especially if it is proprietary or classified

• Interest in matters outside the scope of their duties
Due to the serious nature of an Insider Threat, the DOR asks that:

- All personnel to be mindful of the potential for individuals (such as: employees, contractors, former employees) to use insider knowledge of sensitive agency information (for instance: security practices, systems that hold sensitive data) to perform malicious actions, which could include, but is not limited to, the unauthorized access or re-disclosure of FTI.

You must report all suspected Insider Threats to the Service Desk.
Information Security Incident Management Policy and Plan

Notify the Service Desk immediately in the event of:

- **Unauthorized disclosure** (an event involving the exposure of information to entities not authorized access to the information).

- **Data Breach** (an incident in which sensitive, protected or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so).

- **The discovery of any suspected Security Incident or threat to the Agency.**

---

*Slide Notes*
Staff Security Responsibilities

Slide Notes

Although agency staff members have access to the internet, please remember the following safety precautions:

- Internet usage is monitored for all staff members.
- Do not download any software without prior approval from the Chief Information Security Officer.
- Any approved files downloaded from the internet must be scanned for viruses in accordance with the procedures listed on our Revenue’s Intranet.
- No Federal Taxpayer Information or Confidential information shall be transmitted over the Internet without prior approval of the Chief Information Security Officer. This is to ensure the communication is approved and is sent using approved secure methods.
Staff Security Responsibilities, cont.

- All Internet email accounts, such as Hotmail, Gmail, and Yahoo are prohibited at Revenue.

And when using a messaging system, please remember:

- Confidential information and FTI should only be disclosed to authorized participants with an established business need, and the information must be used for processing a valid business request.

All messages are subject to North Carolina Public Record laws.
Did You Know?

Email sent through your NCDOR email account is considered public record and could be potentially seen by anyone!

Before hitting send, ensure that the information you are sending is something you would be comfortable with the public having access to.

Slide Notes

Did you know emails are considered to be a public record?

Before hitting send, ensure that the information you are sending is something you would be comfortable with the public having access to.
Posting on Social Media regarding an incident is considered indirectly communicating with the media.

The Agency has designated the Public Affairs office as the only department authorized to communicate with the media and to make statements on behalf of the Agency on social media regarding incidents or any other issue.

Slide Notes

Posting on Social Media regarding an incident is considered indirectly communicating with the media.

The Agency has designated the Public Affairs office as the only department authorized to communicate with the media and to make statements on behalf of the Agency on social media regarding incidents or any other issue.
Social Media, cont.

Slide Notes

There are many social media outlets and all are easily accessible. However, unless authorized by the Secretary of Revenue:

- Do not make statements about Revenue using these outlets.

- Staff should never make statements about Revenue on social media or use Revenue logos, letterhead, etc.

- Revenue staff should never make offensive comments or engage in communications that violate the privacy or public rights of others.
Always lock your Computer Screen

You are responsible for any and all activity that takes place under your UserID.

Always lock your screen before leaving your seat or shutdown your computer when it is unattended.

Use the following key combinations:

- Ctrl + Alt + Delete, then press the Enter key on your keyboard
- Ctrl + Alt + Delete, then select Lock at the top of the menu that displays
- Windows + L

Slide Notes

Along with creating and using strong passwords, you can also protect the access of information by locking your computer. Because you are responsible for any activity that takes place under your UserID, it is required that before you leave your seat.

- Always lock or shut down your computer when unattended.

- You can lock your screen by using the following key combinations:
  - Ctrl + Alt + Delete, then press the Enter key on your keyboard
  - Ctrl + Alt + Delete, then select Lock at the top of the menu that displays
  - Windows + L key

By taking these appropriate measures, it will help to safeguard not only yourself, but also taxpayer information.
Mobile Resources (Inside DOR)

You are responsible for the security of any Mobile Resources assigned to you!

Inside DOR Facilities
- Mobile resources are considered secure unless otherwise indicated.

Contact the Service Desk immediately in the event of a device being lost or stolen.

Slide Notes

If any mobile resource has been assigned to you, (e.g., laptops, smart phones, or tablets), you are responsible for its security.

All mobile resources are considered secure while inside Revenue facilities, unless otherwise indicated.
Mobile Resources (Outside of DOR)

Slide Notes

While outside of Revenue facilities, mobile resources should be stored out of plain sight and when possible, under lock and key.

When traveling by common carrier (e.g., airplane, train, bus, or boat) mobile resources should NOT be checked as baggage.
Prevent a System Virus

Best Practices for preventing a System Virus!

- Do not install or connect any non-DOR issued hardware or media to any DOR device or the DOR network.

The only exception is if there is a valid business need and proper precautions have been taken.

Slide Notes

To prevent the possibility of system viruses, do not install or connect any non-Revenue issued hardware or media to any Revenue device or to the Revenue network.

When in doubt, here is an easy way to remember: if Revenue did not issue it to you, do not put it into a Revenue computer. The only exception is if there is a valid business need, and proper precautions, such as virus scanning, have been performed prior to connecting it to the Revenue network.
Prevent a System Virus, cont.

Best Practices for preventing a System Virus!

- Do not install or connect any non-DOR issued hardware or media to any DOR device or the DOR network.

The only exception is if there is a valid business need and proper precautions have been taken.

Slide Notes, cont.

Examples of hardware and media may include:

- CDs
- Modems
- Flash Drives
- MP3 Players
- Personal Data Devices
- iPods
- Smart Phones
External Electronic Removable Media (E-Media)

Best Practices: E-Media

If there is valid business need to receive external electronic removable media (E-Media) from a taxpayer or other state agency:

- The E-Media must be scanned for malicious content before it can be stored or used on ANY DOR Resource.

Slide Notes

If there is business need that requires you to receive external electronic media such as a CD, USB drive, or flash drive from a taxpayer or other state agency, remember that all electronic media must be scanned for viruses before being stored or used on any Revenue system.
Password Best Practices

What You Should Always Do...

- Create passwords that contain at least 8 characters
- Use a unique combination of letters, numbers, symbols, and both upper and lower case characters

Remember, the complexity of your password is nice but the length of your password is key!

Slide Notes

For the safety and security of the data housed at Revenue, our systems require passwords, and in some cases, multiple passwords to access information.

To improve the security of system passwords, they should be complex and contain at least 8 characters utilizing a combination of upper and lower case letters, numbers, and special characters.

Remember, the complexity of your password is nice, but the length of your password is key.
Password Best Practices, cont.

What You Should Not Do...

- Never share your passwords with others
- Never store your password in any electronic communication
- Never embed passwords
- Do not include dictionary words or popular phrases
- Do not use easily guessable combinations such as Spring 2017, October 2017, Password 1, Abcd1234
- Do not use simple adjacent keyboard combinations, such as qwerty, asdzxc, or 123456

Slide Notes, cont.

Below are some more password best practices in regard to password safety:

- Revenue staff should not share passwords with other staff members, store their passwords in any electronic communication, or embed their passwords in automated programs, utilities, or applications.

- Staff should not use words included in a dictionary or popular phrases. System intruders may try to use special tools called “password crackers” that include all dictionary words, and it can be modified to include popular phrases and sports teams to guess your password.
Creating Secure Passwords

Slide Notes

Weak passwords are quite common. The image above provides a list of the most common passwords used in 2019 and are prime examples of passwords that are easily cracked using hacking tools.

Did you know a passphrase is one of the most secure types of passwords and is the recommended method to use when creating a password?

A passphrase is a collection of words that form a phrase or sentence. It’s easy for you to remember but very hard for others to guess. You can add to the complexity by substituting some of the letters for symbols and numbers.
Creating Secure Passwords, cont.

A chain is only as strong as its weakest link. This means a weak password can make YOU the weakest link. Let’s strengthen the chain by doing away with weak passwords.

**Passphrase Examples Only** - Do not use the examples below when creating your own passphrase.

<table>
<thead>
<tr>
<th>Example 1 Passphrase: I would like my password to be very secure!</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Password:</strong> lwIm2bvs! (Notice that the word “to” was substituted by the number 2.)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Example 2 Passphrase: Why does it take so long to come up with a new password?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Password:</strong> Wdits1tcuw@np? (Notice the “a” was substituted for an @ symbol.)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Example 3 Passphrase: The month of October is Security Awareness month!</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Password:</strong> Tmo0iSAM! (Notice the capital “O” was substituted for a “0” [zero].)</td>
</tr>
</tbody>
</table>

**Slide Notes, cont.**

Refer to the password examples provided in the image above but do not refer to them when creating your own passphrase.
Email Best Practices

Slide Notes

The next section in this training discusses some Email Best Practices.
Never respond to SPAM!

**Slide Notes**

It is important that all personnel understand the risks associated with responding to Spam.

**Here are few reasons why you should NEVER respond to Spam:**

- Responding to Spam will let the Spammer know your account is active, then they can pass your information onto other spammers, which will cause a great increase in the amount of spam you receive.

- You should note clicking the “Unsubscribe” link is also considered responding.

- Responding will allow the Spammer to potentially coax you into giving him or her sensitive information.
Never respond to SPAM, cont.

Slide Notes, cont.

- Due to the fact that Spam emails often bear fake source email addresses, by responding you may unwillingly collaborate in a devious scheme meant to saturate the mailbox of some unsuspecting target victim.

- If you believe you have received a Spam message, you should always report it by clicking the Report Phish (Phish Alarm) button from your Microsoft Outlook toolbar – refer to the image below.

- If you are reporting an email from a shared mailbox, forward the email as an attachment to the Service Desk.
Unauthorized Disclosures

One of the most common ways unauthorized disclosures occur is when personnel insert confidential information into an email and then choose Reply All without first checking exactly who the email is going to.

It is always a good idea to check your email at least twice before hitting the send button to ensure that you have reviewed what information you are sending out and who you are sending it to. To avoid this, always verify who you are replying to before choosing Reply All. If you choose Reply All, make sure not to include confidential information.
Phishing Emails

Slide Notes

Phishing emails are getting more sophisticated every day. With some scrutiny, you can spot a phishing email using a few techniques.

Don’t trust display names – They can be easily faked. Always check the email address in the “from field.” If it looks suspicious, don’t open it. Ensure that you are seeing the senders’ email address and evaluate it well.

Look but don’t click – The text of a link is easily editable by the person creating the link. By “hovering” the mouse over the link (essentially moving the mouse arrow over the link but NOT clicking on it), you can see the actual destination of where the link is trying to send you. If it looks suspicious, do NOT click it!
Phishing Emails, cont.

Don’t trust display names

Look but don’t click

Don’t click on attachments

Check for spelling and grammatical mistakes

Slide Notes, cont.

**Don’t click on attachments** – Including malicious attachments that contain viruses and malware have become a common phishing tactic. Malware can damage files on your computer, steal your passwords, or spy on you without your knowledge. Attachments have embedded code that can be executed when the attachment is opened. Do not open any email attachments you were not expecting. Not always, but many times a quick phone call to the sender can help to determine if an attachment is malicious or safe. If you are not expecting the attachment, do not open it.

**Check for spelling and grammatical mistakes** – Another way to identify phishing emails is to check the grammar of the email, especially if the email is from a business. This could be a sign that something is not right. Legitimate messages usually do not have major spelling mistakes or poor grammar. Always read through your emails carefully.
Beware of urgent or threatening language in the email – Invoking a sense of urgency or fear is a common phishing tactic. Attackers want you to open the email and click on links and they will try to use tricks like these to do just that.

Beware of subject lines that claim your account has been suspended or your account had an unauthorized log in attempt.

Don't give out personal information – Legitimate banks and most other companies will never ask for personal credentials through email, so do not give them out.
Phishing Emails, cont.

**Phishing Emails, cont.**

- Beware of urgent or threatening language in the email
- Don’t give out personal information
- Review the signature
- Don’t believe everything you see

Slide Notes, cont.

**Review the signature** – When trying to determine if the email is a phishing email, you should always look at the signature. If there is a lack of information about the sender or ways to contact the sender, you may want to evaluate the email more to see if there are any other signs that this is a phishing email. Lack of details about the sender or how you can contact the company, strongly suggest it is a phish. Legitimate businesses always provide contact details.

**Don’t believe everything you see** – Phishers are extremely good at what they do. Just because an email has convincing brand logos, language, and a seemingly valid email address does not mean it is legitimate. Logos and images are easy to copy and paste. Email addresses are easy to create. Always trust your instinct. It is always better to err on the side of caution.

**Be skeptical when it comes to your email messages** – If it looks even remotely suspicious, don’t open it.
**Did You Know?**

The Agency requires that personnel do not include links within internal email messages.

If you receive a confidential identifier (SSN, FEIN, EIN) from a taxpayer, you should remove (or mask) it prior to responding to the email.

**Slide Notes**

The agency requires that employees do not include links within internal email messages. What does this mean for you? If you receive an email with a link, do not click it. You must report the suspicious email to the Service Desk.

If you receive a confidential identifier (SSN, FEIN, EIN, etc.) from a taxpayer, you should remove (or mask) it prior to responding to the email.

Staff should not include full identifiers within email because all email transmissions are considered public records. Not including full identifiers will mitigates the risk of potential unauthorized disclosure(s) in the future.

**NOTE:** Review the examples in the image above of a masked social security number, federal employee identification number, and employee identification number.
Facility Security Policy Reminders

Slide Notes

The next section in this training covers Facility Security Policy Reminders.

- Wear your badge between the neck and waist.
- Report a lost or stolen badge immediately.
- Never share your badge.
- Escort visitors at all times.
- No piggybacking or tailgating.

Slide Notes, cont.

Here are some reminders about facility security policies:

- You should always wear your badge between the neck and the waist. This allows all Staff, including those who are responsible for the security of our building to know who you are and that you are NCDOR staff.
- Always report a lost or stolen badge immediately to the service desk, security guard, or Director of Business Operations.
- Personnel should never share their badge with anyone.
Slide Notes, cont.

- NCDOR visitors must be escorted at all times.

- Personnel should never allow another individual to “piggyback” or “tailgate” through security checkpoints (e.g. doors with badge access).
If you see something, say something!

Slide Notes

Badges are used for more than just access. For example, if a physical security event were to occur at DOR, the state police would be looking for indications of identity (such as badges). The absence of a badge may indicate the presence of someone who is unauthorized to be in restricted areas.

It is important that your badge is visible and that it is worn between the neck and waist. If you are escorting visitors into the building, make sure that they wear their visitors badge at all times!

Tailgating is when someone avoids badging in through a badge reader by following closely or “tailgating” behind staff who have used his/her badge to gain access legitimately. This is a common method that malicious agents use to gain physical access to restricted areas. There should never be a case where someone does not use their badge to gain access to a restricted area.
If you see something, say something, cont.

If you see something, say something!

Slides Notes, cont.

Here are some ways that you can help to prevent this from happening:

- Never hold the door to a restricted area open for someone. They must **always** badge in themselves.

- Never allow someone to use your badge to gain access to a restricted area. If you see someone tailgating or piggybacking through a security checkpoint, let a Security Guard know immediately!

- If you hear a knock on the door (while in a restricted area), do not open it, especially if you cannot see the individual who is knocking!
Alternative Worksites

There may be situations where staff need to use or access Revenue information while away from a Revenue facility. These locations are considered alternative work sites.

Some examples of acceptable work sites may include:

1. A customer’s tax office
2. An employee’s hotel room during official business travel
3. A teleworker’s home office
Alternative Worksites, cont.

Slide Notes, cont.

Even though staff may be conducting official business with a customer, staff is reminded to refrain from accessing or discussing Revenue business in public areas, such as airports or coffee shops.

Discussing Revenue information in these types of locations may put staff at risk of making an unauthorized disclosure of confidential information.
Facility Safeguards

Slide Notes

Safeguards are in place when handling confidential information at the DOR facility and alternative worksites.

Some examples include:

- Update your voice message to inform taxpayers not to leave personal identifiable information (PII, FTI, or STI).
- Be aware of your conversation level as not to be overheard by others.
- Forward business calls to your Revenue issued cellular phone that requires a PIN to retrieve messages.
- Adhere to the agency's clean desk policy. Do not leave documents on your desk when not present.
Slide Notes

Interruptions and distractions could result in consequences such as:

- Sending information to the wrong person. For example, forwarding an email to the wrong person or sending taxpayer information to the wrong taxpayer.

- Visible screens and uncovered paperwork have the potential to be seen by individuals who are not authorized.
Thank You!

For questions regarding the information covered in this eModule, contact the IT Security team at (919) 754-2323.

Slide Notes

You have reached the end of the 2020 Information Security and Privacy Awareness training. If you have questions regarding the information covered in this training eModule, contact the IT Security team at (919) 754-2323.