

Indiana Department of Revenue

Security & Privacy Awareness

Training

2026



Contents

Introduction	4
What are the sources of this training?.....	4
Who Does this training?.....	4
Why do we take this training?	4
Physical Security.....	5
Physical Security: Conclusion	6
Data Security	6
Data Security: Conclusion	7
Types of Information	7
Types of Information: Conclusion	8
Authorized Access & Disclosure of Information	8
Authorized Access & Disclosure of Information: Conclusion.....	9
Penalties.....	10
Penalties: Conclusion	11
Labeling & Sending Information	11
Labeling & Sending Information: Conclusion.....	13
Storage & Disposal of Confidential Information	13
Storage & Disposal of Confidential Information: Conclusion	15
Phishing.....	15
Ways to Recognize Phish.....	17
Phishing: Conclusion	18

Social Engineering 18

Ways to Recognize Smish 18

Social Engineering: Conclusion 19

Insider Threats 19

Insider Threats: Conclusion..... 20

Working Away From the Office 21

Working Away From the Office: Conclusion 23

Security Precautions for IT Staff..... 23

Security Precautions for IT Staff: Conclusion 25

Finally 26

Introduction

Welcome to the Indiana Department of Revenue's Security and Privacy Awareness Training.

The Indiana Department of Revenue, or DOR, handles a large quantity of information. Millions of Hoosiers and taxpayers across the country trust us to keep their Social Security numbers, home addresses, bank account numbers, and other information we receive about them secure. While we are legally and professionally obligated to protect this information, we also know it's the right thing to do.

What are the sources of this training?

The material you will learn by completing DOR's Security and Privacy Awareness Training comes from a variety of sources, including the IRS, Indiana Code, state policies, and even DOR policies.

Who Does this training?

Whether you're a full-time employee, a contractor, a vendor, or hold a different position, we're all part of Team DOR. Many of us work with taxpayer and customer information. Some of us work with data about our information systems and infrastructure. And even if you don't work directly with any sensitive data, in any DOR office, you are always steps away from documents that contain sensitive information, computers through which sensitive content can be accessed, and within earshot of conversations about sensitive topics. Remember, as members of Team DOR, we have a duty to protect the sensitive information with which we are entrusted.

Why do we take this training?

In the wrong hands, the information we work with can be used to harm and embarrass taxpayers, businesses, our teammates, DOR, and the State of Indiana. Individual and business taxpayer information can be used to commit tax fraud and identity theft and cause financial damage. Information about the vulnerabilities of our information systems and infrastructure can be exploited to publicly embarrass DOR and the state, weakening taxpayer confidence in us.

By learning about and adhering to the policies and procedures discussed in this training, DOR team members demonstrate integrity and commitment to service, driving our agency toward fulfilling our mission.

Completion of this training meets IRS, state, and DOR requirements and serves as your agreement to adhere to the policies and procedures to which we are bound.

Physical Security

At DOR, our photo ID badges and office security protocols work together to enhance the physical security of our teammates, our customers, and our information.

All teammates are assigned photo ID badges, which allow us to access and enter secure spaces like parking garages, Indiana government buildings, and DOR offices. We must never share them with anyone. If your ID badge is lost or stolen, report it to your supervisor right away.

The IRS requires us to clearly display and wear our ID badges above our waists. This also allows us to easily and readily identify who should be in our offices and who should not. All visitors, even DOR teammates visiting an office other than their assigned district office, must sign the Visitor Log and wear a badge. Visitors who are not DOR teammates must be accompanied by a DOR teammate. If an unknown person without a properly displayed DOR or visitor badge asks to be let into badge or key-access areas during office hours, direct them to one of the following five options, depending on the circumstance:

- The Central Office receptionist desk.
- The Ameriplex Suite P entrance security office.
- The senior person at your District Office.
- Their manager if they are an employee.
- The person they are visiting if they're not an employee.

If someone asks for this access after-hours, try to verify whether they're entitled to that access, and let them in only if you have made that verification. If not, guide them to the reception area to sign the Visitor Log and wait for their DOR host.

Do not attempt to escort uncooperative, belligerent, or threatening persons from secured areas. Instead, dial 911 and immediately notify your supervisor.

We must always scan our badges when entering secured spaces. DOR policy prohibits piggybacking/tailgating, that is, "allowing others to enter DOR office spaces without scanning their badges."

While it's okay to hold the door open for another DOR teammate, we must always ask them to scan their badge before entering. This helps ensure only authorized personnel have access to DOR spaces.

When you enter or exit DOR spaces, make sure the doors close completely and lock behind you. Report doors that don't close or lock correctly to your supervisor.

If you were assigned keys to access DOR offices or storage spaces, please protect them. Never make a duplicate key without authorization. If you need a duplicate key or your key is lost or stolen, inform your supervisor immediately.

Physical Security: Conclusion

At DOR, your physical security comes first. By following the procedures discussed in this training, we can help to keep our workplaces, teammates, customers, and information safe.

Remember to always wear your badge above your waist and scan your badge every time you enter a DOR space. Never allow someone else to use your badge.

If you are a DOR key holder, keep your assigned keys secure. Never make a duplicate key without authorization.

If you need a replacement badge or key, or if either is lost or stolen, report it to your supervisor immediately.

Data Security

Our computers contain applications that house sensitive information. So, how can you help improve DOR's data security?

Bad actors are continuously trying to access our state computers and network. One of the easiest ways they can do this is by figuring out our passwords and using them to log into our accounts. To stop them from being successful, we must use long and complex passwords. Our passwords must be no less than 16 characters long, and contain at least one uppercase letter, one lowercase letter, one number, and one special character.

If someone asks you to share your password, don't! You should be the only person who knows your password because if someone else gets it, uses it to log in as you, and does damage, you could be held accountable.

If we leave our state computers unlocked when stepping away, we are inviting others to view information they likely have no authorized access to. In some cases, the people who might view this information are insider threats—bad actors who happen to be DOR staff.

Whether people have the best of intentions or are maliciously trying to access information in an unauthorized way, it is our responsibility to prevent that access by ensuring our computers are locked when not in use.

Hold the Windows key and press the L key to lock your computer.

If we see an unlocked computer left unattended, we should do our teammate a favor and lock the computer for them. Doing so demonstrates our core value of teamwork.

When we need to share our state computer screens with others, we should always ensure we are only showing relevant content. For example, we wouldn't want to accidentally show a sensitive email, a customer's tax return data, or details about DOR's systems to those who don't have the proper credentials.

Protecting printed materials is important to data security. To keep another person from taking what you print, retrieve the documents immediately.

Data Security: Conclusion

Most of us work on state computers every day, so it's easy for us to see them as only work tools. However, to a bad actor, they are gateways to sensitive systems and data. That's why we must prevent others from accessing them.

Always lock your state computer if you step away from it, whether you're in the office, at home, or another location.

Whenever we share our screens, we must ensure we are not showing data that others should not and are not authorized to see.

Types of Information

Daily, we access many types of information, including Social Security numbers, tax-related legal documents, bank account numbers, and more.

At DOR, we classify information into three categories: non-sensitive, sensitive, and confidential.

- Non-sensitive information does not require protection. This could include public newsletters and tax guidance.
- Sensitive information requires some protection. It must only be shared with people who are authorized and have a need to know.
- Confidential information requires maximum protection. It must only be shared with people who are authorized and have a need to know. Additionally, it must be stored and sent securely.

For more guidance on sensitive and confidential information, refer to the [Securing Sensitive Information Job Aid](#).

Federal Tax Information (FTI) is any information DOR receives from the IRS or another federal source. Remember, all FTI is confidential.

Types of Information: Conclusion

The primary purpose of this module is to help us understand the three classifications of data we use at DOR and how to protect it.

Refer to the [Securing Sensitive Information Job Aid](#) which can be used as a reference for the information provided in this section.

If you are not sure how certain information should be classified and secured, check with your supervisor or the DOR Security team.

Authorized Access & Disclosure of Information

DOR teammates are able to see a lot of information, even some we don't need to perform our jobs, so it's important we only view the information we're supposed to. Additionally, DOR must share certain information with other organizations, such as law enforcement and government agencies, the public, and, of course, our customers. To ensure the best information security, we must understand and follow the rules to view, handle, and share data with others.

There are two important terms we use at DOR to discuss viewing and handling taxpayer and customer information: "access" and "need to know."

"Access" is the ability to use, view, receive, or work with information. "Need to know" means there is a clear, job-related reason for accessing it.

You may only access taxpayer information if you have a "need to know." Browsing or looking at taxpayer information out of curiosity is not permitted. You may access information about other DOR personnel only if you are assigned this task in the normal course of your work. If a coworker approaches you asking for help with their own tax matter, refer them to the Taxpayer Advocate Office, also known as T A O. All DOR teammates—including contractors—who need help with their Indiana individual, or business tax accounts must contact T A O by emailing EmployeeTaxQuestions@dor.in.gov. Personal inquiries must not be sent through IN-TIME messaging.

You must not access your own information. Your family and friends must contact DOR in the same manner as any other customer and not through you. If you happen to come across information belonging to a family member or friend in the normal course of your job, notify your supervisor as soon as possible.

It's important to remember that even if you are authorized to access information, you must only use it for official DOR purposes. DOR teammates are never allowed to personally gain from the information they learn in

the course of their work at DOR. Even after our employment ends, we are all legally accountable for maintaining the security and privacy of the information we learn while working at DOR.

If it is part of your job responsibilities, you may provide information to:

- The customer or taxpayer you are assisting.
- The customer's or taxpayer's representative with a completed Power of Attorney (POA-1) form.
- An authorized individual listed on a return (but you can only discuss information relating to that specific return); or
- Other DOR teammates with a clear job-related need to know.

If you're working with a business, you can discuss information with responsible officers or contact persons listed with DOR, or an authorized representative with a POA-1 on file with DOR.

Never provide sensitive information to:

- A friend or family member of a customer who is not an authorized Power of Attorney; or
- An employee of a business customer who is not a responsible officer or the Power of Attorney.

Now that we've discussed access and need to know, let's talk about disclosure. Disclosure is when a DOR teammate provides taxpayer information to a third party.

If you're asked to provide taxpayer information to someone other than those we just discussed, contact the appropriate Disclosure Officer via the list housed on DORway.

Authorized Access & Disclosure of Information: Conclusion

We must respect our customers' right to privacy and only share information with those who have the proper access and need to know.

Browsing or looking at customer information out of curiosity and accessing the data of other DOR teammates (unless you are assigned this task in the normal course of your work) are all strictly prohibited. Accessing your own data is always prohibited.

All DOR teammates who need help with their Indiana individual or business tax accounts must contact the T A O at EmployeeTaxQuestions@dor.in.gov. Friends and family members of DOR teammates must contact DOR through normal customer channels for help.

If it's a part of our assigned job responsibilities, we can provide information to authorized individuals. If we're asked to provide information to others without a need to know, contact a Disclosure Officer. If we're asked to disclose information and it is not within our normal duties, we should reach out to a Disclosure Officer.

Penalties

Any unauthorized access, disclosure, or inspection of state or federal tax information (FTI) is a serious violation of agency policies and state and federal laws regarding the protection of customer privacy.

Teammates who violate these policies and laws are subject to disciplinary action which may include termination of employment and—depending on the severity of the offense—civil lawsuits and criminal charges.

- Unauthorized access or disclosure of confidential Indiana state tax information can result in a Class C misdemeanor, punishable with a fine of up to \$500 and/or up to 60 days in jail.
- Unauthorized inspection of FTI is a federal misdemeanor, punishable with a fine of up to \$1,000 and/or up to 1 year imprisonment plus the costs of prosecution.
- Unauthorized disclosure of FTI is a federal felony, punishable with a fine of up to \$5,000 and/or up to 5 years imprisonment plus the costs of prosecution.
- Offering and receiving any item of material value in exchange for FTI is a federal felony, punishable with a fine of up to \$5,000 and/or up to 5 years imprisonment plus the costs of prosecution.

If you knowingly or negligently inspect FTI or disclose FTI to someone who is not legally authorized to receive it, you can be sued by the customer whose privacy was violated. In this case, civil penalties will apply, and if you are found liable, you would have to pay the customer the greater of:

- (a) \$1,000 for each act of unauthorized inspection or disclosure, or
- (b) The total of the actual damages the customer suffered because of your actions plus punitive damages in certain instances plus the customer's attorney's fees.

Incidents of unauthorized access, inspection, and disclosure of sensitive and confidential taxpayer information are data breaches and are serious security issues that must be addressed as soon as possible. When we learn of a data breach, we must immediately report it, as directed by DOR guidance and federal and state laws, even if it was accidental, seems minor, or does not appear to have resulted in harm to a customer.

Your help is needed to report unauthorized access and disclosures to the DOR Security Team. This allows DOR to fulfill its responsibility to the IRS and affected citizens. With this information, the IRS Office of Safeguards works with DOR to notify and help impacted taxpayers, and to inform them of the corrective actions taken to hold the people who caused the breach accountable.

Those responsible for causing data breaches can face a range of state and federal punishments that could include written reprimands, change of positions, loss of pay, and even termination of employment.

Teammates should use one of the two following options to report incidents:

1. Report an incident to DOR's Security Team at IDOR_Security_Office@dor.in.gov
2. If you feel more comfortable reporting the incident to an outside agency, you can report it directly to the IRS Office of Safeguards.

Remember, once you become aware, report any known or suspected improper access or disclosure of sensitive information. As teammates, we must work together to protect information that has been entrusted to us.

Penalties: Conclusion

Your help is needed to report incidents of unauthorized access, disclosure, and inspection of information. Report these incidents to the DOR Security Team so DOR can fulfill its responsibility to the IRS and affected citizens.

Teammates can also report incidents of unauthorized access, disclosure, or inspection of FTI directly to the IRS Office of Safeguards.

As teammates, we must work together to protect information that has been entrusted to us.

Labeling & Sending Information

The IRS requires DOR to adhere to heightened protections when handling FTI. These requirements are outlined in IRS Publication 1075.

DOR has identified specific teammates as the authorized personnel to request and receive FTI directly from the IRS in the form of TDS (Transcript Delivery System) transcripts or electronic data extracts. These authorized personnel provide other DOR teammates with FTI when needed and help ensure all FTI procedures are being followed.

When authorized personnel provide DOR teammates with printed TDS transcripts, they will place a label on the information identifying it as FTI and advising them of the penalties for unauthorized disclosure. These printed documents must be returned to the authorized personnel for logging and shredding.

Whenever possible, we should not make printed or electronic copies of FTI. If your work does require that you make a copy of FTI, that copy must be labeled and logged as a new copy of FTI and then tracked until it is properly destroyed. Discuss with your supervisor whether your job requires you to copy FTI on a regular basis.

Per IRS Publication 1075, we must log all FTI from receipt to destruction. At a minimum, FTI Logs must include a taxpayer identifier (e.g., name), the relevant tax year (or years), the type of FTI used (e.g., 1040), how the FTI

was used, and the dates the FTI was received and destroyed. We must not include FTI in the log. If FTI is included, the log must be maintained in a secure location, like a locking file cabinet or with a designated FTI Team. Contact DOR's Compliance and Ethics team if you have any questions about FTI Logs and for assistance with creating an FTI Log.

Refer to the [Securing Sensitive Information Job Aid](#) for any questions on the types of information which should be sent securely.

In addition to the protections already discussed, there are a few other steps we need to take when sending FTI.

If you need to send FTI by mail, use two envelopes or a sealed box for transport. When using two envelopes, clearly mark the inside envelope as "confidential." The outside envelope or box should not say "confidential."

When we mail any type of confidential information, it is vital to double-check that the name and address are correct, and that we do not accidentally include extra pages meant for a different customer with the confidential information.

If you discover that confidential information was accidentally disclosed to the wrong person, immediately let your supervisor know. Then report the matter to the DOR Security Team.

If you send an email containing FTI, treat it like all other confidential information, and only send it using DOR's secured email. In addition, the secure email must contain a subject line that begins with "FTI." These emails are tracked and logged to ensure that DOR follows IRS requirements.

When responding to an email, be sure to review your message for confidential customer information, Personally Identifiable Information (PII), or other items that may be subject to disclosure restrictions or protections.

No additional precautions are necessary for emails containing only a customer's name and email address.

Never fax FTI. If you inadvertently send a fax containing FTI, immediately let your supervisor know. Then report the matter to the DOR Security Team.

We should never include confidential information in any form of social media, including platforms like LinkedIn and SuccessFactors JAM.

Labeling & Sending Information: Conclusion

The IRS requires DOR to adhere to heightened protections when handling FTI.

If your work requires you to make a copy of FTI, that copy must be labeled, and logged, as a new copy of FTI and then tracked until it is properly destroyed. Discuss with your supervisor whether your job requires you to copy FTI on a regular basis.

When we mail any type of confidential information, it is vital to double check that the name and address are correct.

When responding to an email, be sure to review your message for information that may be subject to disclosure restrictions or protections. No additional precautions are necessary for emails containing only a customer's name and email address.

We should never include confidential information in any form of social media, including platforms like LinkedIn and SuccessFactors JAM.

Notify your supervisor immediately if you discover:

- Confidential information was inadvertently or intentionally disclosed to the wrong person.
- Confidential information was disclosed improperly.
- Mail containing FTI was not sent in accordance with DOR policy and IRS regulations.
- An email containing FTI was not sent encrypted and with a subject line that begins with "FTI".
- FTI was faxed.

Then, report the matter either to the DOR Security Team or the IRS Office of Safeguards.

Storage & Disposal of Confidential Information

When storing and disposing of confidential information, we must observe heightened security procedures.

At DOR, confidential information that is stored digitally can only be permanently stored in designated databases or secure storage spaces approved by the DOR Security Team. If necessary and if we have a need to know, it's okay to save the information temporarily on our state-issued laptop or desktop computer hard drives, because they are appropriately encrypted. However, we must remove that information as soon as we no longer need it to complete our job-related tasks.

We must never store electronic FTI documents in Microsoft OneDrive, and we must never save FTI to our Documents, Desktop, or Pictures folders, as they back up to OneDrive. When we download documents from

emails or browsers, they are automatically saved in our Downloads folder, which is an inappropriate location for long-term FTI storage.

There are only three approved locations where you can securely store electronic FTI:

1. Microsoft Teams designated for Confidential FTI: FTI can be stored in Confidential FTI Teams if you need to work with it long term.
2. Email: FTI can be stored in your Outlook account if the messages containing FTI are secured with Office 365 Message Encryption (O M E). When you no longer need the information, delete the emails from the folder they are in, and then from the Deleted Items folder.
3. Hard Drive: FTI can be temporarily stored in a folder located on the hard drive of your state-issued computer.
 - a. Launch File Explorer.
 - b. Select This PC, then Windows (C:).
 - c. Create a new folder and name it "FTI".
 - d. Temporarily save FTI documents in this folder until you no longer need them.
 - e. Delete documents you no longer need and empty your Recycle Bin.

You are not permitted to store confidential information on removable digital media like CD's, DVD's, USB flash drives, etc. With that in mind, you might receive confidential information on removable digital media from external sources. If this happens, label the media appropriately to ensure we know what's stored on them, like FTI or PII. After labeling, transfer the data to a secure location. Then, contact the DOR Security Team for guidance on the disposal of such storage devices.

It is a violation of policy to store confidential information digitally on personal equipment or on non-secured shared drives, sites, or servers. If you're unsure if a digital storage location is appropriate for storing confidential information, check with your supervisor or the DOR Security Team.

In addition to digital materials, we must also follow specific rules for storing confidential information contained in printed materials. FTI must be separated from non-FTI as much as possible to prevent accidental disclosure. If separating FTI from non-FTI in paper documents is impractical, label the entire document as FTI. If the printed materials contain confidential information other than FTI, label it as such.

Users should not leave confidential information unattended or unprotected. When we're not actively working with it, we must ensure it is secure. Ensure your computer is locked when not in use, and store confidential information in a secure location such as a locked filing cabinet. Make sure the key to the cabinet or container is kept in a separate location.

When we no longer need confidential information, we must dispose of it in very specific ways. Disposal includes shredding, purging digital files from removable media, and more.

- CD's or DVD's containing FTI should be taken to the DOR Security Team for disposal.
- CD's and DVD's not containing FTI can be placed in a locked shred bin.

- Contact the DOR Security Team for advice and assistance with the disposal of all USB devices.

The disposal method for printed materials depends on the type of information it contains.

- TDS transcripts containing FTI are provided only by authorized DOR teammates who are responsible for tracking those documents. When you no longer need a TDS transcript, you must return it to the DOR team member who gave it to you.
- Printed material that may contain FTI must be placed only in the DOR-provided, locked shred bins.
- Printed material that does not contain FTI may be disposed of either by shredding in a DOR-provided shredder, or by placing the material in any locked shred bin.

Remember, as DOR team members, we serve our customers—and each other—by protecting the confidential information with which we are entrusted. Storing and destroying it in accordance with the DOR policies and procedures mentioned here will help protect that information and prevent it from getting into the wrong hands.

Storage & Disposal of Confidential Information: Conclusion

As DOR teammates, we must always honor our responsibility to protect confidential information. When storing and disposing of it, we must observe heightened security procedures.

It is a violation of policy to store confidential information digitally on personal equipment or on non-secured shared drives, sites, or servers. If you're unsure if a digital storage location is appropriate for storing confidential information, check with your supervisor or the DOR Security Team.

Users should not leave confidential information unattended or unprotected. When we're not actively working with it, we must ensure it is secure.

Remember, as DOR team members, we serve our customers—and each other—by protecting the confidential information with which we are entrusted. Storing and destroying it in accordance with the DOR policies and procedures mentioned here will help protect that information and prevent it from getting into the wrong hands.

Phishing

Social engineering done via email is called “phishing,” and it is the most common form of social engineering seen at DOR.

To protect our computers, systems, and information, we must be able to identify phishing attempts.

Refer to the [Is It Phish Job Aid](#) when faced with a potential phishing attempt.

Don't open attachments or follow links in emails that may be phish.

Once we know an email is phish, we should report and delete it. Report the email following the instructions on the IT & Security page on our inDOR intranet.

Social engineering is the tactic of manipulating, influencing, or deceiving a victim in order to gain control over a computer system or steal personal and financial information. Its goal is to trick users into making security mistakes or giving away sensitive information. Social engineering done over email is called phishing. We need to understand how to recognize and report phishing to prevent ourselves, and others, from falling for it.

DOR team members are often the target of phishing attempts. Some of these emails try to trick us into selecting links that lead to bad sites and launching attachments that are actually malware, software intended to damage a computer system.

Those who fall for these schemes unintentionally cause their computers to become infected, introducing security risks to our systems, the state network, and the data belonging to our customers and coworkers.

The effects of malware can be immensely damaging. Viruses can change and destroy our files and programs. Spyware can be used to watch our computer activities, enabling bad actors to see personnel and taxpayer records that should be kept private.

A certain kind of spyware called keylogger enables bad actors to see and record what you type, like Social Security numbers and passwords you use to log into our most sensitive applications. You may have recently heard about ransomware that is designed to lock our files until we pay bad actors to unlock them.

Victims of malware must have their computers fixed, often leading to productivity loss and the deletion of project files.

Some bad actors pretend to be different people, asking seemingly innocent questions. When this information is put together, however, these people then have a better understanding of our organization's structure and practices. Separately, these emails appear harmless, but the information collected from them all could enable bad actors to gain unauthorized access.

You also may have heard of "spear phishing." This is where a bad actor specifically targets you because of your access to systems or data.

DOR has also seen phishing emails that pretend to be from people we know, using a technique called spoofing. To do this, bad actors send us emails that forge the identities of our leaders, supervisors, and coworkers as the senders. Bad actors hope that if we see emails from people we know, we'll immediately do what they want us to (like select a malicious link), leading to increased risk and loss of security.

For emails that appear spoofed, we can call or message that person to see if they really did send it. If they tell us they didn't send it, then it's phishing.

Ways to Recognize Phish

- Urgent call to action or threats
 - Bad actors will often entice you to act swiftly, hoping you will make a mistake and inadvertently grant them access to our computer systems.
- Unknown, first time, or senders marked "External Email"
 - While not an immediate indication of a phishing attempt, it's important to slow down and ensure the person who emailed you is legitimate.
- Spelling or grammatical errors
 - Some of these mistakes may be accidental, but some bad actors use spelling and grammar mistakes to attempt to evade spam protection filters.
- Generic greetings
 - Often, reputable businesses and organizations know your name; be wary of generic greetings like "Hello system user."
- Mismatched email domains
 - Check the email address of the sender; if they claim to be from DOR, for example, their email domain should be dor.in.gov. Some bad actors will alter the domain so it's similar: dor.in.com.
- Suspicious links or attachments
 - When you hover your cursor over a link, it should be the same address. For example, if the link is www.dor.in.gov, it should show the same address in the hover window. Check the address showing and look for small differences. For example, www.in.dOr.com.

Once we know an email is phish, we should report and delete it. Always follow the most up-to-date instructions on DORway when reporting email as suspected phish.

When the IOT Security Team receives notifications of phish, they can adjust the state's email filters to block them from reaching anyone else's state email accounts. When the DOR Security Team is notified of phish, they use it to determine if they should send an agency-wide message to tell everyone to beware.

Phishing is an ongoing threat. Download the "Is It Phish" document and keep it for regular use. It's our responsibility to keep DOR's and DOR's customers' information secure.

Phishing: Conclusion

Social engineering done via email is called “phishing,” and it is the most common form of social engineering seen at DOR.

To protect our computers, systems, and information, we must be able to identify phishing attempts.

Refer to the [Is It Phish Job Aid](#) when faced with a potential phishing attempt. Don’t open attachments or follow links in emails that may be phish.

Once we know an email is phish, we should report and delete it.

Social Engineering

While phishing is the most common form of social engineering seen at DOR, it isn’t the only kind. Social engineering can also occur through text message, phone calls, and in person.

Smishing is social engineering performed through text messages. The goal of smishing is the same as phishing—to trick victims into giving up sensitive information or clicking on links they shouldn’t. To determine if a text message is smishing, we can use most of the same methods we use to identify phish. If we conclude a message is smish, we should simply delete it. If the sender continues to text us, we can block the number.

Ways to Recognize Smish

- Link to an unknown site.
- Message from an unknown sender.
- Requesting you verify your identity.
- Sender claiming to be a reputable source.
- Urgent call to action.

Social engineering can also be done by phone call. This is called vishing, and it’s like phishing and smishing. Bad actors disguise themselves as someone legitimate, luring and scaring their targets with rewards or threats, hoping they disclose information they shouldn’t. They may claim to be from the IRS, informing us that they will send law enforcement to arrest us unless we pay a balance with a credit card, for example. Bad actors may pretend to be from DOR’s or IOT’s IT staff to convince us to provide them with information about our computers. If you get suspicious calls like these, do not tell them anything. Instead, take note of the date and time of the call, the number they are calling from, and the information they are requesting before you hang up. After that, email that information to the DOR Security Team with the subject “Phone Scam.”

Social engineering can also be done in person. Because of the work we do, the data we handle, and the systems we manage, there may be bad actors bold enough to approach us in person to attempt to learn more information about our agency. They may also try to trick you into introducing malware onto your computer or phone, offering you a flash drive to plug into your device or suggesting you download certain software. To ensure we don't reveal any information, simply decline their requests for information. If they insist on getting this information, get their name and contact information, and tell them you will give it to someone at DOR who may be able to help them. When you have the chance, report everything you know about the person.

Making the mistake of trusting a stranger could lead to stolen data and damaged equipment and systems. If you think someone is trying to social engineer you, report everything you know about the person and their request to your supervisor.

Recognizing and reporting social engineering attempts is the responsibility of everyone associated with DOR. Stay vigilant!

Social Engineering: Conclusion

Our role as public servants requires us to be vigilant and make smart decisions to protect customers' and teammates' information.

Be mindful of social engineering attempts made through text, phone, and in person. Take time to pause and consider what is being asked of you before taking any actions. When in doubt, contact the DOR Security Team for guidance.

Everyone is at risk of becoming a victim of social engineering attempts. By practicing the knowledge and skills learned here, you can help prevent yourself from falling for malicious schemes designed to steal information.

Insider Threats

We often think about security as protecting ourselves against threats outside of DOR. We may assume that all our teammates adhere to DOR's core values; however, this isn't always true. There is a possibility that people who work alongside us may seek access to data, applications, and systems that they shouldn't have. These people present insider threats to our organization.

An insider threat is the potential for DOR team members to use their authorized access or understanding of the agency to harm us. We must learn to recognize, assess, and report insider threats as necessary.

So, what motivates someone to be an insider threat? Some are driven by curiosity and want to know personal information about people like former significant others or celebrities. Other insider threats are compelled to

wrongdoing by need because they've fallen on hard times. There are also those who may want to sell what they can access for personal gain. And then there are insider threats who just want to harm DOR.

The motivations of insider threats affect their behaviors, leading them to break organization policy or state and federal law. While insider threats often try to hide their bad actions, there are strong indicators that someone is an insider threat. Look for someone who:

- Intentionally views data for which they have no legitimate business reason to access.
- Tries to physically remove large quantities of files or computing components from DOR.
- Tries to electronically transfer large quantities of data by uploading it onto thumb drives or into a cloud storage service.
- Insists on obtaining access that they don't need for their job responsibilities.
- Verbalizes the ability or intent to harm DOR or its teammates.

If you observe any of these behaviors, notify your supervisor and the DOR Security Team immediately. We want to create a work environment in which we hold ourselves and each other accountable, identifying and reporting those who intentionally aim to break rules and compromise our security.

Individuals who are insider threats do not live up to our core values that make DOR the nation's premier tax administrator and a great place to work.

To prevent ourselves from falling victim to insider threats, we should follow all the procedures previously discussed in this course. That includes locking our computers when not in use, keeping our passwords secure, and securing and disposing of sensitive information appropriately.

Remember that security is a responsibility we all share, and that includes keeping DOR safe by identifying and reporting insider threats.

Insider Threats: Conclusion

Security is a responsibility we all share.

While most DOR teammates are committed to living out our core values, the threat of an insider still exists. In the wrong hands, the data and information collected by insiders could cause immense harm to our customers and our agency. We must be able to recognize, assess, and report insider threats.

Look for the key behaviors that may indicate someone poses an insider threat. If you observe any of these behaviors, notify your supervisor and the DOR Security Team immediately.

To prevent ourselves from falling victim to insider threats, we should follow all the procedures previously discussed in this course. That includes locking our computers when not in use, keeping our passwords secure, and securing and disposing of sensitive information appropriately.

Working Away From the Office

Some DOR teammates are allowed to work remotely when operational needs are best served that way and when approved by the Commissioner and/or someone they designate. Approved remote work must be performed within Indiana unless traveling outside the state for official functions and expressly authorized by your management chain, the Commissioner, and Cabinet Secretary. If you plan to travel outside Indiana and take your equipment with you, fill out the “Out-of-state Work / Equipment Authorization” form, obtain all approvals, and follow the remaining instructions

When we work remotely, we’re not operating in controlled environments like DOR facilities. There are no locked doors requiring us to scan our badge, confirming those around us are DOR teammates, and there are no cameras to monitor what happens to our sensitive information. For these reasons, we must practice very different security when working away from the office.

It’s important to know that official DOR work must be done on state-issued or DOR-approved computing devices. These devices have been determined to have the necessary security safeguards to access DOR email, applications, and data. Using personal computers or public computers, like the ones in hotels or libraries for example, to perform agency work could risk our systems and information.

We must also ensure our laptops have current updates and patches. While IOT deploys them, we must ensure they are properly installed. To do this, we watch for emails about patching sent by the DOR ITD and Communications Teams and follow the instructions to ensure our computers stay up to date.

When working away from the office on our state-issued laptops, we must follow two steps to access the secure state network: first, we must have Internet access, then we must log into the state network using the state-standard VPN tool. This will help prevent bad actors from intercepting sensitive data and DOR applications we may access on our state-issued laptops. If you work outside of DOR spaces and do not yet have a VPN account, you should ask your supervisor to request one for you immediately.

You are not permitted to use personal smartphones, tablets, or computers to access the following:

- The statewide secure network.
- Microsoft Teams, Outlook and other applications managed by the state.
- DOR email accounts through synced applications.
- DOR applications like ITS and MCS.

This prohibition does not include the Okta app. You are permitted to have that on your personal phone.

When working from home, it is highly encouraged that we secure our wireless network by requiring a long and complex password to log in and implementing any other security measures recommended by our Internet

service provider. If our home Wi-Fi network is not secure, then bad actors could access it, any devices connected to it, and any data going over it.

If you're working away from the office or your approved remote working location, using public Wi-Fi networks like the ones at coffee shops, airports, hotels, and libraries is highly discouraged, as it could allow bad actors to easily access your state-issued laptop. If you have a state-issued phone, you can access the secure state network by configuring it to act as a mobile hotspot, then connecting to that secure network. Contact the DOR Security Team for instructions on how to do this.

When traveling in cars, planes, or buses, we should always keep our bag or briefcase with us and ensure we have it with us when we exit. DOR has had several reported instances where laptops have been stolen from vehicles. When traveling by car, it's best to keep your computer bag and other DOR materials in your trunk. If your vehicle doesn't have a trunk, then you can cover your belongings with a blanket or jacket. Hiding them well keeps them out of sight of bad actors.

We must practice good physical security when working away from the office, whether at a customer's location, a conference, or even at home. Make sure that unauthorized people are unable to view our sensitive data.

When at a customer's location or conference, we should ensure no one is behind us looking at our laptops or papers. When we break for lunch or plan to be away for an extended period of time, it's good security practice to take our bag containing our laptop and papers with us. If we leave our laptops behind, we should lock the screen and make sure the location is secure. In the end, we must make decisions based on which actions result in the lowest risk.

We must practice security even when working at home because family members and friends, although we know them, are still not authorized to view DOR data. Consequently, we can't show them anything we're working on or leave any work items subject to their review. As you would at a customer's location or conference, make sure no one can see your laptop screen or papers. When you're finished working, shut your computer off, secure your papers and other work materials, and lock them away from anyone's access.

If after practicing all this security, we still end up a victim of a security incident, we must report it as soon as possible. If you contract malware, please reach out to IOT first, then inform your supervisor, and have your supervisor contact the DOR Security Team.

If you lose your laptop or other work materials, or if they are stolen, file a police report immediately, then notify your supervisor and have them contact the DOR Security Team.

Remember that working away from the office presents increased risk, so we must be aware of our surroundings and practice the appropriate security to protect the computers and sensitive data for which we are responsible.

Working Away From the Office: Conclusion

When working away from the office, it's vital that we observe heightened security practices.

Completing work on our state-issued computers, ensuring our devices receive security patches, and logging into the VPN tool will help DOR's data remain safe.

When traveling, be sure to keep your computers and other work documents with you or in a secure location.

Be vigilant and use sound judgment. If you have any questions or concerns, contact the DOR Security Team for further information.

There's one more thing and it's about Artificial Intelligence better known as AI. Unless you are specifically permitted to use authorized AI tools like the IOT Managed Microsoft Copilot apps on your work equipment.

State and DOR policies prohibit you from downloading and using unauthorized AI tools and apps on your work computer and work phone.

The reason for this is that many unapproved AI tools are too risky. They may not protect confidential information the way we need it to. Or they may generate wrong information, which if shared could misinform people and lead to bad decisions.

If you think you need an AI tool ask your supervisor first and if they agree you should have it your supervisor should submit a software request at the DOR service desk that's accessible from the inDOR homepage.

Security Precautions for IT Staff

Those of us who work in DOR IT may have additional access permissions that other agency teammates don't have. Some of us have access to computer code, scripts, servers, and data. Others can change security settings and configurations, and some plan and manage the technical architecture of DOR systems. Because some of us have exceptional access permissions and knowledge of our infrastructure, we must exercise additional security precautions.

IT teammates who handle the following types of data should take extra care to protect it:

- Firewall rules.
- IP addresses.
- Network/system architecture diagrams.

- Vulnerability scan results.
- Standard hardware and software configurations.
- Application code.

We must only share this information with those who have a need to know. Sharing this data on social media sites or message boards, for example, is strictly prohibited. If you use social media platforms, be careful not to share anything that would compromise the sensitivity of our systems, taxpayer information, or our reputation as an agency.

When troubleshooting problems with vendors, we should provide them with the minimum data necessary, even if it isn't sensitive.

If you're a developer or database administrator, you may need to download and test software. When these situations arise, there are several reasons why you should not immediately download, install, or launch software.

1. First, the software may not comply with the security standards to which DOR must adhere. Using it may make DOR non-compliant with IRS and state requirements.
2. Second, the software may have flaws, vulnerabilities, and embedded threats that could introduce risk to DOR and the state.
3. Third, it may introduce licensing problems to DOR. Some free software is permitted for personal use and not for use in large organizations like ours.

In the event you need to download software for business purposes, you should first check with your supervisor. If they approve, then your supervisor should send the request to the ITD Service Desk. The Service Desk team will then either help you obtain and install the software if it's already approved by DOR or propose another solution to meet your needs.

Developers should be aware that their codes may be vulnerable to threats like SQL injection and cross site scripting. In production, vulnerable code can be exploited to permit bad actors' access to our systems and data. To reduce this risk, developers should follow the guidance prescribed by the most current version of the DISA STIG checklist for application security and development. Developers with questions about this should contact the DOR Security Team.

DISA stands for: Defense Information Systems Agency. STIG's stands for: Security Technical Implementation Guides (STIG's).

Any IT teammate who needs to perform administrative activities must always do so with their elevated accounts. For example, anyone who logs directly into a server without using a client, starts and stops servers

and databases, or pushes code to or makes code changes on servers, should only do so using their elevated account. Doing this will ensure our compliance with IRS guidance.

IT teammates must remember never to browse from, or access emails, while logged directly into servers. Doing so could contract malware onto servers that could damage them, or it could allow sensitive data hosted on them to be stolen.

System owners and managers should also take extra security measures. They should know what service accounts their systems use and ensure the associated permissions are at the appropriate level for what needs to be done. For example, service accounts with administrative privileges will put the entire system at risk in the event it is compromised.

If you believe a system or data has been compromised, contact the DOR Security Team immediately for assistance. Do not try to fix the problem on your own.

Remember, as IT teammates, we possess a great deal of IT information that can be used by bad actors to defeat DOR's security. As a result, we must do everything necessary to prevent that from happening. And if our security is compromised, we must make the DOR Security Team aware immediately so they can provide the guidance and assistance necessary to address it.

Security Precautions for IT Staff: Conclusion

As IT team members, we possess information which can be used to exploit our agency and the information entrusted to us. We must only share this information with those who have a need to know.

Any IT teammate who needs to perform administrative activities must always do so with their elevated accounts. Doing this will ensure our compliance with IRS guidance. We must remember to never browse from, or access emails, while logged directly into servers. Doing so could contract malware onto servers that could damage them, or it could allow sensitive data hosted on them to be stolen.

If you believe a system or data has been compromised, contact the DOR Security Team immediately for assistance. Do not try to fix the problem on your own.

We have been entrusted to keep DOR's IT systems and data secure. Following the procedures outlined in this training allow us to live out our core values of integrity and respect.

Finally

Your commitment to protecting DOR's data speaks volumes of your dedication to our core values. Well done!

Completion of this training meets IRS, state, and DOR requirements and serves as your agreement to adhere to the policies and procedures to which we are bound.

Thank you!