DAS EIS

Department of Administrative Services
Enterprise Information Services

Information Security Training - 2022

Next

Introduction

Information Security is a topic that is vital to our work environment but also and just as importantly, to our personal lives, our families and our communities. We encourage you to take the information gleaned from this training and use it to inform those close to you of the cyber risks they may encounter in their daily lives.

While cybersecurity has a strong focus on the technology tools we all use, it's our behavior and how we use the technology that determines the cyber security risk.

Security culture is most effective when everyone cooperates as a team to engage in good security practices as a matter of habit and routine. It is both a mindset and mode of operation.

Each time you do things, like log into your computer, check your email, use your phone or access our systems when volunteering/working from home you connect to a network of assets that we depend on for our operations.

Your attention to security best practices is critical to reduce risk and keep our organization safe. Our number one defense against theft and loss is you.

Thank you for being an integral part of the state of Oregon's security team.

Next

Objectives

- Identify the types of security threats that put consumers' personal information at risk.
- Recognize the manipulative social engineering techniques that criminals use to access sensitive information.
- Identify the best methods for minimizing security risks in all forms of electronic communication.
- Identify the best practices for using cloud services.
- Identify the steps to take to regain access after you've been hacked.
- Recall the guidelines and best practices required for creating a secure home office.
- Recognize best practices that minimize the risks to sensitive data that are created when using a personal device for work activities.
- Identify ways to reduce risk to data through minimization.
- Identify the password best practices that keep our information secure.
- Identify ways to limit access to your mobile device and laptop computer while volunteering/working remotely.
- Identify the need to report security incidents when volunteering/working remotely.

Next

Safe Computing - Threats

We face a rising number of threats that could compromise the security of our information and resources. Threats and incidents may be caused by malicious attempts to steal information, but more often they are caused by simple inattention to policies and procedures. Either way, you have the power to stop most security threats.

Although the number of security threats is endless, the most common categories are:

- Loss: Misplacing a resource or device.
- Theft: Stealing information—electronically or physically—or resources.
- Cybercrime: Damaging electronic devices, files, or our organization's network.

We've developed security policies and procedures designed to help you combat these threats. Your attention to these policies and procedures is critical to preventing actions that could lead to security breaches.

Next

Safe Computing – Threats
Cybercrime

Any crime that involves a computer and a network. It can occur as a result of:

- Connecting to unsecure Wi-Fi networks.
- Neglecting to update computer software.
- Clicking links in a phishing e-mail.
- Sending sensitive or confidential information in an unencrypted e-mail.
- Opening e-mail attachments from unknown sources.
- Posting sensitive or confidential information to social networking sites.

Next

Safe Computing – Threats
Theft

Theft can occur as a result of inattention to security procedures. Theft can occur as a result of:

- Leaving work resources in unlocked locations or unattended while in public places.
- Leaving work resources in briefcases, purses, clothes pockets, or on desks around the office.
- Leaving documents containing sensitive information in plain view for unauthorized individuals.
- Allowing unauthorized individuals to access our secure facilities.
- Being tricked by social engineering scams.

Next

Safe Computing – Threats
Loss

Information that is transportable can be lost. Security breaches can occur as a result of losing:

- USB drives.
- Laptops.
- Documents.
- DVDs.
- Briefcases or purses.
- Tablets.
- Smart phones.

Next

Safe Computing – Threats

Social Engineering

Whether over the phone, through electronic communications, or even face to face…social engineers are con artists that exploit our emotions to steal information. No technological defense can truly protect us from social engineering, because you, staff and other volunteers are the target.

It's up to you to spot the con and take the right actions to stop social engineering scams.

Next

Safe Computing – Threats

Social Engineering Techniques

These are examples of just some of the most common social engineering techniques. Remember that thieves may try these scams to target ODFW or you personally.

Over the Phone

- Posing as a reputable service provider.
- Impersonating a government or law enforcement official.
- Pretending to be a customer to extract account information.

In E-Mail

- Impersonating individuals of authority within our organization.
- Messages threatening you with financial penalties.
- Warnings of suspended accounts that require you to enter your credentials.
- Smart phones.

In Person

- Individuals posing as service technicians or delivery person hoping to enter our facility.
- Pretending to be a potential client hoping to glean information from your computer screen.
- A fake job interviewee assessing our organization.

Exploiting Emotions

- **Fear**
- **Sympathy**
- **Trust**

Next

Safe Computing – Threats
Summary

In this lesson, you learned we face various computer threats that compromise the security of our information and resources. Your attention to safe computing practices is the best way to combat these threats.

Take a moment to review the key points covered.

- Be aware of varying security threats that can put our information and resources at risk.
- Social engineers use a variety of manipulation techniques to access sensitive information, usually by exploiting fear, sympathy, or trust.

Next

Safe Computing – Principles

Electronic Communications

Electronic communications—such as e-mail, instant messenger, texting, and social networking services like Facebook, Twitter, and LinkedIn—make it easy to communicate. However, along with the convenience comes the risk of a security breach. Once information reaches the Internet, it is virtually impossible to recall or delete.

You are the first line of defense in ensuring the security of personal and sensitive information that we handle. Your actions have far-reaching consequences, which is why it's so important that you follow our processes when using electronic communication technologies.

Next

Safe Computing – Principles
Cloud Services

Cloud services and apps give us the ability to instantly share content between coworkers, customers, and vendors; but they also expose us to increased risk of data leakage or information compromise. Though we do review the security practices of approved vendors, it's always best to be cautious and

keep security in mind when exchanging any business information with external parties.

Next

Safe Computing – Principles
I’ve been hacked!

Even if you've taken all the recommended precautions to protect your information and your devices, you can still fall victim to hacking. If you think you've been hacked, there are several important steps you should take to ensure you can regain access to your accounts and keep hackers out!

Take a moment and learn about hacking and some techniques to regain control.

- Determine how they got in. Hackers use several techniques including malware, phishing, social engineering, and attacking internet sites to access your information.
  - Malware: Malicious software that can infect your computer or network.
  - Phishing: Fraudulent messages sent by scammers.
  - The Internet: Stealing information that you’ve entered on unprotected sites.

Next

Safe Computing – Principles
I've been hacked!

- **Determine how they got in**. Hackers use several techniques to access your information including:
  - Malware: Malicious software that can infect your computer or network.
  - Phishing: Fraudulent messages sent by scammers
  - Social engineering: Manipulation techniques to access sensitive information, usually by exploiting fear, sympathy, or trust.
  - The Internet: Stealing information that you've entered on unprotected sites.

Next

Safe Computing – Principles
I've been hacked!

- **Reset your password**. The easiest step to take in regaining access to your account is to reset your password. Be sure your new password is:
  - A combination of symbols and numbers.
  - Not similar to any old passwords.
  - Frequently changed.

Password reuse creates liability for your computer and information. Because you've been hacked, it's more urgent that you change your password for all accounts that may have been hacked or affected.

Next

Safe Computing – Principles
I've been hacked!

- **Review your risk profile**. Hackers often use malware and phishing to get your information, but they also attach internet sites and steal information from accounts where you've reused your password.
  - Using the same password for all of your accounts makes your accounts and information vulnerable to attacks.

- **Monitor other accounts**. Hacking puts both you and your contacts at risk. After an attack you should alert your contacts
  - Some hackers assume your identity and contact your friends and family to request money and maybe more. Once you've regained access, let your contacts know you've been hacked – this will put them on high alert for any suspicious activity that comes from you or your account.

Next

Safe Computing – Principles

I've been hacked!

- **Know who you put at risk**. Oftentimes the hacked account provides a path to other accounts that may be vulnerable. After an attack you should treat all accounts as thought they've been compromised.
  - Monitor your back accounts for unauthorized purchases or transfers.
  - Double check all shipping addresses and payment methods.
  - Lock down your credit to prevent identify theft.

- **Look for Backdoors**. Once you've regained access to your accounts, check for backdoors designed to let a hacker back in. Smart hackers set up tools to make sure they can access your account even after you've gotten them out. Be sure to check and update your e-mail rules, filters and security questions and answers.

Next

Safe Computing – Principles
Summary

In this lesson, you learned that we face various computer threats that compromise the security of our information and resources. Your attention to safe computing practices is the best way to combat these threats.

Take a moment to review the key points covered.

- Apply our electronic communications guidelines, such as encrypting e-mails and verifying the source of hyperlinks you receive, to keep both our customers' and your information secure.
- Cloud services must be used with best practices in mind, such as being on guard for phishing attempts and maintaining compliance requirements when sharing data, to prevent the compromise of sensitive information.
- If you fall victim to hacking, there are several important steps you should take to ensure you can regain access to your accounts.

Next

Safe Remote Computing

Your Home Office

Volunteering/working from home has some great advantages. You can skip the commute, avoid office distractions, and stay in your pajamas; however, it can also expose our company information to increased risk because your home office doesn't benefit from the numerous electronic and physical security controls of our corporate location. We trust you to be productive when working at home, and also trust you to think carefully about making your home office as secure as possible.

Next

Safe Remote Computing

Your Home Office

Secure Your Home. Take common-sense measures to ensure that your home is secure from unauthorized entry.

- Lock your doors and windows before leaving.
- Do not leave your computer or other valuable equipment in plain sight.
- Place work devices in a concealed and preferable locked location when not in use.
- Do not post your status as volunteering/working from home on social media accounts.
- Engage in voice conversations where others cannot overhear.

Next

Safe Remote Computing

Your Home Office

Home Life. Whenever possible, distance your work duties from domestic responsibilities.

- Do not allow children, your spouse, or even your cat to touch your work devices.
- While volunteering/working, limit other devices, such as various “smart” appliances or other computers, from connecting to your home network.
- Do not leave important company documents where they could be accidentally thrown away or damaged.
- Use a cross-cut shredder to dispose of any documents that contain sensitive information – never your family garbage can.
- Do not insert personal peripheral devices, like USB drives, smartphones, cameras, or other gadgets into your company computer.

Next

Safe Remote Computing

Your Home Office

Protect your router. Take the time to configure your home router's setting to maximize security.

- Change the administrative password from the manufacturer's default.
- Turn off SSID broadcast to limit who can detect your network.
- Turn on MAC filtering so that only specified devices can connect to the router.
- Disable remote management features, if available.
- Regularly check for updates to the router's firmware.

Follow our organization's controls. Treat your work computer with the same level of security consciousness when at home as you are expected to when at work.

- Use a password and lock your computer's screen when away.
- Access only the information you need to complete the work for which you are currently responsible.
- Keep antivirus and firewall software up to date and running.
- Use a VPN to connect to our network.
- Save files to our designated cloud server.
- Encrypt files and messages when appropriate.

Next

Safe Remote Computing

Mixing Business and Personal

When you use your personal device for both work and personal activities, it's important to ensure that your personal use doesn't compromise our business information. Inappropriate use of your device—like ignoring our security procedures—turns it into a skeleton key for data thieves. Without the proper security controls, your mobile device can be used by cyber-criminals to access both your personal information and our proprietary data.

Next

Safe Remote Computing

Mixing Business and Personal

Accounts. Modern web services have no shortage of accounts that require sign-in. Keep the following best practices in mind:

- Never use your personal username and password as the credentials for a professional account, and vice versa.
- Never use your personal device for business use.

Cloud storage. Remote storage is a great way to extend the space on your device or back up your data; however, keep the following practices in mind before your start using a cloud service:

- Never backup our organization's information to unapproved cloud-based services, such as Dropbox, Google Drive, or iCloud.
- Never use our organization's cloud-based service to store and/or backup your personal information.

Remember: Backing up your personal data is exclusively your responsibility. If your device is lost or compromised, you must report it immediately. IT will wipe your device and information that has not been backed up may be lost.

Next

Safe Remote Computing

Mixing Business and Personal

Apps. There may be an app for just about everything, but that doesn't mean you should use the same app for both personal and work purposes. For example:

- Refrain from downloading apps that have not been approved by IT.
- Use different apps for work e-mail and personal e-mail.

Data Minimization. Data minimization is all about reducing risk to the information we handle. This means thinking carefully about collecting, accessing, and retaining the least amount of data necessary. Keep an eye out for opportunities to minimize data exposure, and help your coworkers do the same.

Remember:
Check with IT to see if third party applications can be implemented to further isolate our organization's data from your day-to-day use of the device.

Next

Safe Remote Computing
Summary

Security threats—actions that put our information at risk—can be caused by malicious activity, but are more often caused by inattention to policies and procedures. Our policies and procedures are designed to protect our information, our resources, and our reputation, but they only work if we all follow them.

Remember, you are our best defense against information theft and loss, so be sure you know and follow our policies and procedures. Now, take a moment to review the key points covered.

- If volunteering/working from home, you must take steps to ensure that your office is secure.
- You can reduce the risk posed to sensitive data by minimizing the amount of date you collect, access, and retain.

Next

Safe Mobile Computing

Remote Incident Reporting

When you’re volunteering/working remotely, you're even more vulnerable than usual to cybercrime. If you notice something unusual or even if you only suspect that an incident has occurred, it's vital that you contact our IT department right away.

Next

Safe Mobile Computing

Password Best Practices

So you've created a strong password? Well, password security doesn't stop there! Every day you and your co-workers make password-related decisions that either keep your password safe, or put it and our data at risk. Password Best Practices:

- Don't use the same passwords for work and home accounts. Variety is better.
- Never share your password.
- If you suspect your password has been compromised, change it immediately.
- Don't write down your passwords or store them electronically.
- Use a password manager if available.
- Set your devices to unlock only by entering a password or pin.

Next

Safe Mobile Computing

Remote Incident Reporting

What is an incident? An incident is any actual or potential compromise of our organization's information or devices. Common examples include:

- Stolen laptop or mobile device.
- Unauthorized access to your hotel room, home office, or home network.
- Erratic behavior of laptop or mobile devices.
- Sensitive information overheard during a private conversation by an unauthorized individual.
- Sending or receiving information over an unsecure network.

Next

Safe Mobile Computing
Summary

In this lesson, you learned that we face various computer threats that compromise the security of our information and resources. Your attention to safe computing practices is the best way to combat these threats.

Take a moment to review the key points covered.

- Follow password best practices to keep our organization's information secure.
- You are responsible for limiting access to your mobile devices and laptop computer while volunteering/working remotely.
- Security incidents, actual or suspected, that are encountered while volunteering/working remotely must be reported immediately.

Next

Quiz time

Let’s see what you’ve learned

Next

Choose the Correct Answer

Which of the following actions could make our sensitive information vulnerable to cybercrime?

A Connecting to secure wireless connections.

B Opening e-mail attachments from unknown sources.

C Refraining from posting information about our organization on your personal social networking sites.

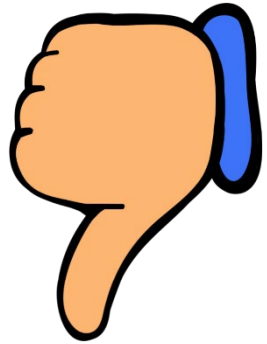
D Keeping security software up-to-date.

That’s right !

Continue quiz

That’s incorrect !

The correct answer is B. Opening e-mail attachments from unknown source could make sensitive information vulnerable to cybercrime.



Try again

Continue quiz

Choose correct answer

Which of the following actions could result in loss or theft of personal information?

A Carrying a laptop on your person at all times when traveling.

B Keeping track of your USB drive at all times.

C Loaning an unauthorized person, such as a messenger or visitor, your security bade to our building.

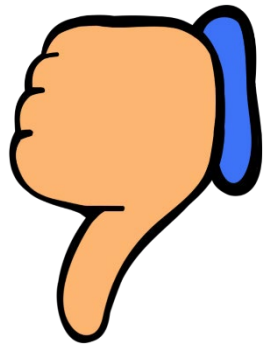
D Discussing sensitive information only in a private setting so passersby cannot overhear the conversation.

That’s right !

Continue quiz

That’s incorrect !

The correct answer is C. Loaning an unauthorized person, such as a messenger or visitor, your security badge to our building could result in loss or theft of personal information.



Try again

Continue quiz

Choose Correct Answer

Which could be a warning sign of social engineering?

A Ambiguous messages requiring clarification.

B Any communication from individuals outside our organization.

C Unsolicited message appealing to your fear, sympathy, or trust.

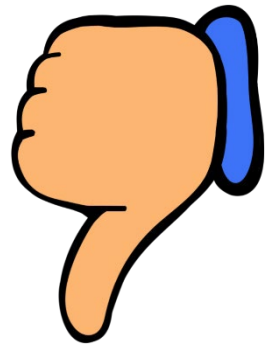
D Customers, clients, or business partners with foreign accents.

That’s right !

Continue quiz

That’s incorrect !

The correct answer is C. Unsolicited message appealing to your fear, sympathy, or trust could be a warning sign of social engineering.



Try again

Continue quiz

Choose Correct Answer

Which of the following forms of communication can experience social engineering?

A Any form of communication.

B Telephone.

C Electronic messages.

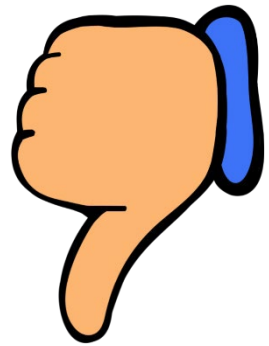
D In person.

That’s right !

Continue quiz

That’s incorrect !

The correct answer is A. Any form of communication can experience social engineering.



Try again

Continue quiz

Choose Correct Answer

Verify the source of any electronic communication that contains a hyperlink.

This includes communication via:

A E-mail.

B Instant messenger.

C Texting and social networking.

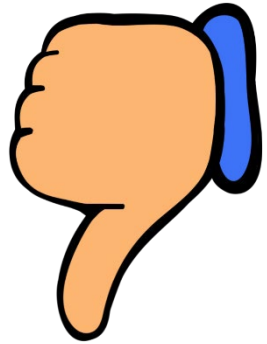
D All of the above.

That’s right !

Continue quiz

That’s incorrect !

The correct answer is D – all of the above. E-mail, instant messenger, texting and social networking all contain hyperlinks.



Try again

Continue quiz

Choose Correct Answer

Once you have posted information to the internet, you can always retrieve or delete it.

A True

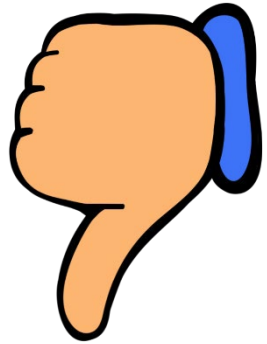
B False

That’s right !

Continue quiz

That’s incorrect !

The correct answer is B – False - Once you have posted information to the internet, you can’t retrieve and delete it.



Try again

Continue quiz

Choose Correct Answer

Look out for which security threat specifically when using a cloud-based service?

A Expired passwords.

B Out of date security software.

C Using only the cloud-based storage to save your files.

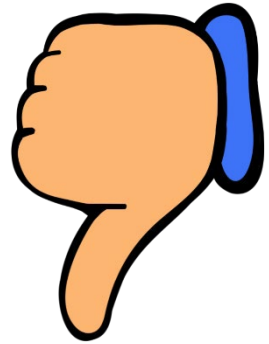
D Phishing attempts from people impersonating a third party.

That’s right !

Continue quiz

That’s incorrect !

The correct answer is D. Look out for phishing attempts from people impersonating a third party when using a cloud-based service. s the information subject to compliance requirements.



Try again

Continue quiz

Choose Correct Answer

Which should be a security consideration before sending sensitive information using a cloud-based service?

A Has the information been fact-checked?

B Is the information subject to compliance requirements?

C Do you have prior experience working with the recipient?

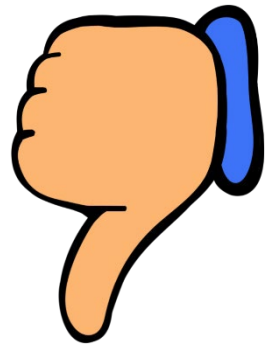
D Is the recipient in a different time zone?

That’s right !

Continue quiz

That’s incorrect !

The correct answer is B. Before sending sensitive information using a cloud-based service you should consider if the information subject to compliance requirements.



Try again

Continue quiz

Choose Correct Answer

If you fall victim to hacking, the only step you need to take to regain access to your account and prevent another attack is to alert the IT department:

A True.

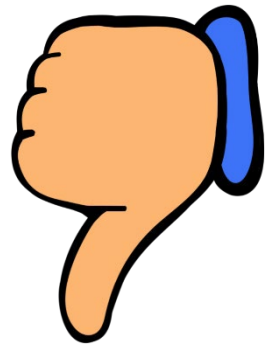
B False.

That’s right !

Continue quiz

That’s incorrect !

The correct answer is B - False. If you fall victim to hacking you should determine how hackers got in, reset your password, review your risk profile, monitor other accounts and look for backdoors.



Try again

Continue quiz

Choose Correct Answer

Which of the following steps should you take to prevent hackers from gaining access to your accounts?

A Use a reputable antivirus software and keep it up-to-date

B Use a secure password and change it frequently.

C Use different passwords for each of your accounts.

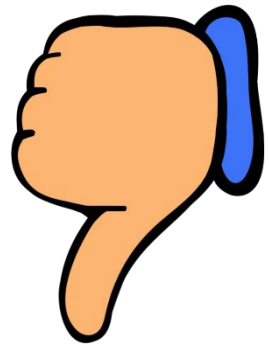
D All of the above.

That’s right !

Continue quiz

That’s incorrect !

The correct answer is D – all of the above. Use a reputable antivirus software and keep it up-to-date, use a secure password and change it frequently, and use different passwords for each of your accounts to prevent hackers from gaining access to your account.



Try again

Continue quiz

Choose Correct Answer

Which of these activities is recommended when volunteering/working at home?

A Using a cross-cut shredder to dispose of documents.

B Inserting personal peripheral devices into your work computer.

C Allowing family members to use your work devices.

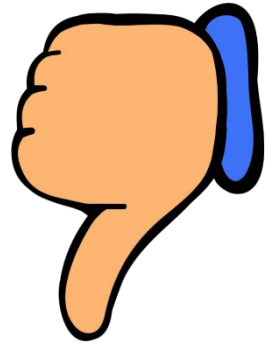
D Connecting “smart” devices to your home network.

That’s right !

Continue quiz

That’s incorrect !

The correct answer is A. Using a cross-cut shredder to dispose of documents is recommended when working/volunteering at home.



Try again

Continue quiz

Choose Correct Answer

Using a VPN to connect to our organization's network is recommended when volunteering/working from home.

A True.

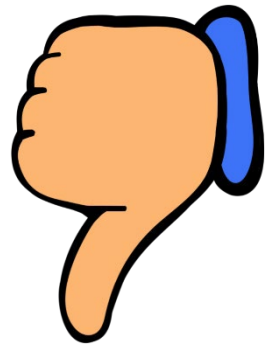
B False.

That’s right !

Continue quiz

That’s incorrect !

The correct answer is A – True. Using a VPN to connect to our organization’s network is recommended when working from home is recommended.



Try again

Continue quiz

Choose Correct Answer

You should use your professional username and password as credentials for a personal account.

A True.

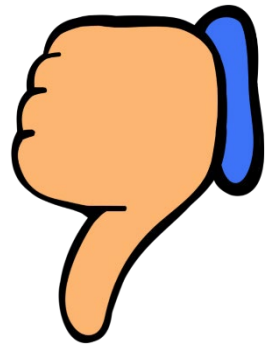
B False.

That’s right !

Continue quiz

That’s incorrect !

The correct answer is B – False. You should not use your professional username and password as credentials for a personal account.



Try again

Continue quiz

Choose Correct Answer

Which is the best definition of “data minimization”?

A Collecting, accessing, and retaining the least amount of information necessary.

B Compressing data so that it fits more efficiently into network storage.

C Editing out unnecessary elements of our policies.

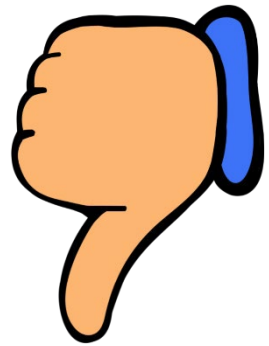
D Possessing too little information to get the job done.

That’s right !

Continue quiz

That’s incorrect !

The correct answer is A. Best definition of data minimization is collecting, accessing, and retaining the least amount of information necessary.



Try again

Continue quiz

Choose Correct Answer

Which best describes the concept of “data minimization”?

A Big data requires big risks.

B Small quantities of data, large levels of efficiency.

C The less data we handle, the less risk we create.

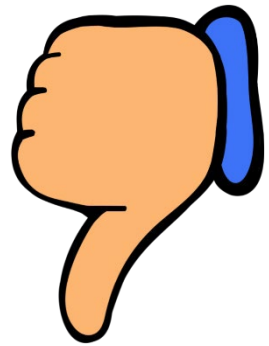
D Minimized data, maximized profit.

That’s right !

Continue quiz

That’s incorrect !

The correct answer is C. The less data we handle, the less risk we create is the best way to describe the concept of data minimization.



Try again

Continue quiz

Choose Correct Answer

Under what circumstances is it most ideal for you to change your password?

A Your coworker gives you a suggestion for a very strong password.

B If your password, or your computer system, has been compromised.

C It’s been at least 90 days since the time you last changed your password.

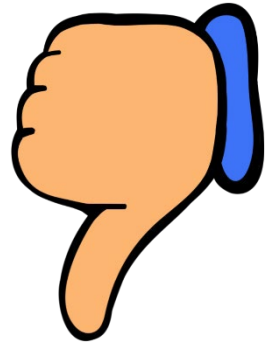
D You’ve heard about a data breach affecting one of your competitors.

That’s right !

Continue quiz

That’s incorrect !

The correct answer is B. It is most ideal for you to change your password if your password, or your computer system has been compromised.



Try again

Continue quiz

Choose Correct Answer

You should share your password only with a member of our IT department, and even then, only when they are in your presence.

A True.

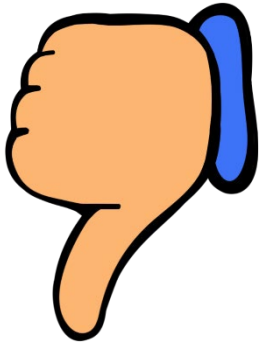
B False.

That’s right !

Continue quiz

That’s incorrect !

The correct answer is B – False. You should never share your password with a member of our IT department.



Try again

Continue quiz

Choose Correct Answer

Which of the following is a good practice for device passwords?

A Use different passwords for each device.

B Store passwords as contacts in a smartphone’s address book.

C Used cached information to recall passwords.

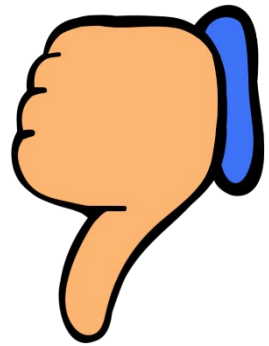
D Keep your password written near your devices.

That’s right !

Continue quiz

That’s incorrect !

The correct answer is A. A good practice for device passwords is to use a different password for each device.



Try again

Continue quiz

Choose Correct Answer

It is unacceptable to let a client or vendor use your device, even if you are watching them.

A True.

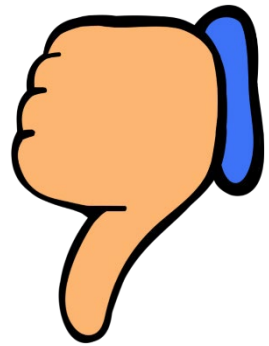
B False.

That’s right !

Continue quiz

That’s incorrect !

The correct answer is A – True. It is unacceptable to let a client or vendor use your device, even if you are watching them.



Try again

Continue quiz

Feedback and/or Questions

- Ask the Supervisor or Manager of the volunteer project
- Ask the ODFW Volunteer Coordinator

ODFW Volunteer Coordinator
Odfw.volunteerprogram@state.or.us
503-947-6413

Resources

- MRD_740_02 Acceptable Use of Information System Assets