Privacy and Security Awareness

Title Screen
<music only>
Over 700,000,000 data records compromised in 2005
*"2015 The Year Breaches Got Personal: Findings from the 2015 Breach Level Index," Gemalto
40% of businesses expect breaches this year
*"Clearswift Insider Threat Index," Clearswift
Average cost of a data breach $3.8 million
*"2015 Cost of Data Breach Study Unites States," Poneman Institute and IBM
30% of breaches are a result of employee error
*"ACC Foundation: The State of Cybersecurity Report," Association of Corporate Counsel (ACC)Foundation
Don't be a statistic
Respect Privacy
Use Caution
Reduce Risk
Build Trust
Be Aware
Privacy & Security Awareness

1: Introduction to Security and Privacy

Information is valuable to our organization. In its many forms, it helps us operate. It can be about what we do and how we do it. And it can be personal information — information about people. Almost everything we do involves information.

Sometimes, the value of information depends on keeping it secret: from the general public, our competitors or even each other. When we do not protect information, we may lose others' trust, weaken our competitive edge or face fines and lawsuits.

When handling information, we *all* must follow laws and policies while also meeting others' expectations. We *all* are responsible for keeping certain information private.

Security—locking and limiting access—can help protect information, but it is only *part* of privacy. **Privacy** is also about *what* information is collected, *how* it is used and *how* it is destroyed.

How can *you* help keep information secure and private? How can *you* protect it from those who would misuse it?

Click on these images for strategies you can apply to help protect information.

Screen 2.1

(Analyze)
Have you ever considered all the types of information you encounter in the workplace every day?

For example, you know the names of the people you interact with at work, but you also might know some of their phone numbers and addresses, details about their personal lives or even some of their financial information.

You know the mission of our organization, but you also might know our strategic plans, trade secrets or clients.

Some types of information require special handling, either because of the law or our own policies. You should determine if any of the information *you* handle falls into this category. If so, you should know the proper procedures to protect it.

When you analyze the information you have access to, and become familiar with what information our organization needs to keep private, you are better able to help protect that information.

(Word cloud of various types of organizational and personal information: Marketing plans, Source codes, Religion, Date of birth, Passwords, Intellectual property, Name, Vacation dates etc.)

Screen 2.2

How did Shana do?

Shana is promoted to a managerial position when Bill retires. When she moves into his office, she finds the filing cabinets are full of old customer files. She figures Bill must have kept the files for some reason, so she will likely need them someday, too. She is sure to lock the files to keep them safe.

Were her actions okay, or not okay? Select your answer and click submit.

Not Ok. Shana should analyze the contents of the cabinets to determine if she needs access to the information contained in the files or if they require any special handling.

Screen 3.1

(Scale down)

Have you thought about all the types of information you *can* access but never or rarely use? Do you really need that information to do your job?

Scaling down the information you access to only what is necessary is one way to keep information from being lost or misused. This could mean limiting access to computer files, physical files or even physical spaces within the organization.

What about the information you share with other people?

Just because *you* can access certain information does not mean *everyone else* should. Before you share information with another employee, be sure they *need* it and have the *right* to access and use it.

When we scale down the information we use and keep, we make it easier to protect the information we need.

Screen 3.2

How did Sam do?

Sam is in charge of supplies and has keys to all of the office closets. HR converts one of the closets into storage for their personnel files in order to better protect them. Sam knows he does not need access to the files and returns his key to the HR Manager.

Were his actions okay, or not okay? Select your answer and click submit.

Okay. Sam made the best choice by returning his key to someone he knew would have the right to access the files.

Screen 4.1

(Secure)

How often do you think about information security? Security is not just about locking the door at the end of the day.

Different types of information require different security measures. Physical items containing information, such as papers and external drives, can be kept in drawers, file cabinets or rooms. These storage areas should be locked, and keys provided to only those people who need access.

Digital protection comes in the form of passwords, firewalls, encryption, anti-virus programs and network protections. While you may not be directly responsible for these measures, there are things you can do to help secure electronic information. If your job requires working on a computer or electronic device, you can:

- Encrypt information when necessary—for example, when saving to a flash drive or emailing it.

- Use secure Internet connections when accessing our organization's network.
- Lock your computer when you step away from it.
- Report suspicious-looking emails. Do not reply to them or open any links or attachments.
- Ask for help with these or any other important security measures.

In addition, passwords are key in protecting electronic information. Ensure that you use strong passwords, store them safely, and replace them if compromised or when directed to do so. It is important to take your organization's password policy seriously and follow it closely.

Just taking a few extra moments to follow security measures keeps valuable information from falling into the wrong hands and being misused.

Screen 4.2

How did Dominic do?

When leaving his workspace, Dominic places a folder containing a customer's financial information in a desk drawer to protect it from those who should not have access to it.

Were his actions okay, or not okay? Select your answer and click submit.

Ok, but… Dominic was correct to put the folder away; however, because of the information it contains, it should be stored in a locked place.

Screen 5.1

(Destroy)

When you dispose of information, do you know for certain it cannot be recovered?

Simply placing a paper document or digital file in the trash does not permanently get rid of it. Cross-shredding, digital shredding and wiping are a few ways to completely destroy information.

The destruction of protected information should be so complete that the most savvy hacker or thief cannot find a trace of it.

However, before you destroy information, *be sure* you are not required by law, regulation or policy to keep it.

Screen 5.2

How did Saul do?

Saul has checked his shipping labels against a printed list of names and addresses to make sure all the labels printed. He is done with the list and throws it in the trash.

Were his actions okay, or not okay? Select your answer and click submit.

Not okay. Saul needs to properly destroy the information by shredding it or by putting it into a locked to-be-shredded bin.

Screen 6.1

(Stay alert)

Have you ever noticed something that you thought might be a privacy issue? Did you know what to do about it?

While we as an organization *try* to protect against problems that might arise, there are always new threats that come with changes in technology, policies or procedures. You are one of the best resources we have in spotting these potential issues.

You are not expected to understand every law or know how to solve every problem. However, to help us protect information, you *do* need to:

- Be aware of our organization's policies and know who to talk to if you have questions.
- Understand the different measures we have in place to protect information, and know when to use them.
- And if you spot a privacy issue, report it to your privacy point of contact.

Screen 6.2

How did Vicky do?

Vicky's workspace is across from the conference room, and she cannot help but overhear a Human Resources meeting regarding an employee's behavior. Later, she is careful not to discuss what she heard with her coworkers.

Were her actions okay, or not okay? Select your answer and click submit.

Okay, but… Vicky was correct to keep the information confidential. She also should inform Human Resources and her privacy point of contact that she is able to hear meetings happening in that room.

Screen 7

Who is responsible for keeping information safe? In many cases, you are. Our organization depends on you to make decisions that will protect all our valuable assets, including information.

When you analyze, scale down, secure and properly destroy information, you help us achieve our goal of protecting it. When you stay alert, you ensure that we continue to guard against potential threats.

Be certain you understand these measures and how they apply to you. Use them to keep information safe.

And remember, you are not in this alone. If you have questions or concerns, ask your privacy point of contact for help.

Congratulations! You have completed the unit.