BUREAU VERITAS

BUREAU VERITAS

Secura

A BUREAU VERITAS COMPANY

THE SAFE PROGRAM

E-LEARNING LIBRARY CONTENT

INFORMATION SECURITY (1/2)

LEARN

Introduction to information security (19 min)

Technical measures are only a part of the solution for an effective information protection policy. The way in which employees handle company information is at least as important. Each employee can be the target of cyber criminals. In this program, you will follow 2 colleagues during their workday. From early in the morning until late in the evening they come across incidents that we can all recognize from a regular day in the office. These practical examples teach you how to deal with such situations.

After the training, you will be able to answer the following questions:

- How do you treat information with care?
- What do you do when you see a suspicious situation?
- How do you handle passwords safely?
- What are the rules of clear desk, screen & office?
- How do you handle visitors?
- How do you recognize suspicious emails?
- How do you print sensitive information safely?
- For what do you use a Virtual Private Network (VPN)?
- How do you work safely in public?

PRACTICE

Clear desk, screen & office (8 min)

You never know who walks past your desk when you are not there. Therefore, never leave any sensitive information unsupervised. This applies to both information on your screen and information on your desk. Lock your computer and do not leave any sensitive information behind when you leave your workstation. Not even if you are gone for just a little while. In just more than a minute, you will learn why a clear desk, screen and office policy contributes to a secure organization.

After this module you will be able to answer the following questions:

- Why do you have to keep your work space clean and tidy?
- What are the dangers if you do not do this?
- How do you prevent these dangers?

ANCHOR

Ransomware (1 min)

Ransomware is a well-known form of malware and is often in the news. Ransomware asks for ransom money to remove a blockage of a computer or computer system. The thing is that you can never be certain if the blockage will actually disappear if you pay. It is better to reduce the chances of getting ransomware. In this training, you will learn about the ways in which you can make the chances of getting ransomware as low as possible.

After the training you will be able to answer the following questions:

- What is ransomware?
- How do you reduce the chance of getting ransomware?

BUREAU VERITAS

INFORMATION SECURITY (2/2)

LEARN

Cybersecurity for Executives (8 min)

Executives and managers play a crucial role in information security. In this introduction training, you not only learn why cybersecurity is important and how you handle cyber risks, but also get practical tips to protect the organization against cyber threats. After completing this training you can create a plan yourself, with which you can start working right away.

After the training you will be able to answer the following questions:

- What is cybersecurity?
- Why is cybersecurity important?
- Which cyberattacks are directly aimed at executives and the management?
- How important is cybersecurity for your organization?
- Which measures does your organization need?
- How do you work on cybersecurity within your organization?
- What do you do in case of an incident?

PRACTICE

Strong passwords (3 min)

We all know that we have to use strong passwords, because weak passwords are easy to guess. When a cybercriminal has got his hands on a password, he has access to confidential information. This awareness video teaches you how you can create strong passwords, what the dangers of a weak password are and how you manage your passwords in a secure way.

After this training you will be able to answer the following questions:

- What is a strong password?
- How do you ensure that your password is easy to remember, but difficult to guess?

Report security incidents (3 min)

Security risks occur daily within your organization. At first glance, they seem innocent, but these risks can lead to incidents. If you think there is an incident or suspicious behavior, it is important that you take action. Your organization will then take the necessary security measures. This awareness video teaches you how to prevent incidents and correctly deal with suspicious situations.

After the awareness video you will be able to answer the following questions:

- What exactly is a security incident?
- What do you have to do exactly when an incident occurs?
- What else can you do to guarantee the security of information?

ANCHOR

Use of passwords (3 min)

The security policy starts with a good password. Strong passwords ensure that unauthorized people do not have access to sensitive information. This microlearning explains in a few minutes what the risks of using passwords are and how you create a strong, easy to remember password.

After the training you will be able to answer the following questions:

- How do you create passwords that are easy to remember?
- How do you securely manage all your different passwords?

Report information security incidents (3 min)

Everyone in an organization can encounter an information security incident. Always immediately, take action if you feel that something is not right and report incidents. This is how you ensure that your organization can quickly take action. This microlearning shows what an information security incident is and how you respond to such an incident.

After the training you will be able to answer the following questions:

- What do you have to do if you notice something unusual?
- What do you have to do if you see that company properties are missing?
- How do you prevent information security incidents?

BUREAU VERITAS

INFORMATION CLASSIFICATION

LEARN

Information classification (10 min)

Working with information is a large and important part of an organization. It is therefore important that you classify information the correct way. This is how you indicate which protection levels are necessary. Everyone then knows which levels of confidentiality, integrity and availability apply when working with the information. The purpose of this is that information does not get lost or end up in the wrong hands.

After the training you will be able to answer the following questions:

- What is information classification?
- Why is it important?
- How do you classify information?
- How do you handle classified information?

PRACTICE

Information classification (4 min)

Working with information is an important part of an organization. By correctly classifying information, you indicate which protection level is necessary. Everyone then knows which levels of confidentiality, integrity and availability they must apply when they are working with the information. The purpose of this is that information does not get lost or end up in the wrong hands. This awareness video explains why it is important to correctly classify every bit of information.

After the awareness video you will be able to answer the following questions:

- Why is it important to correctly classify information?
- What are the most common classification types?
- What are the dangers of losing information of a certain classification type?
- What do you have to do if people ask for information?

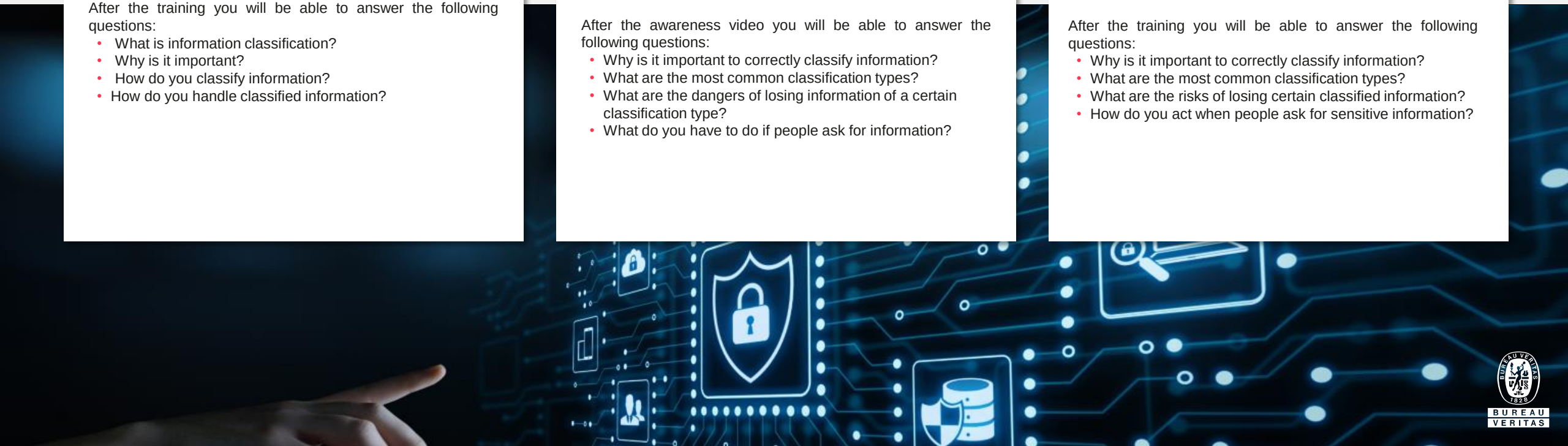
ANCHOR

How is information classified? (3 min)

Working with information is an important part of every organization. By correctly classifying information, you indicate which protection level is necessary. Everyone then knows which levels of confidentiality, integrity and availability they must apply when they are working with the information. The purpose of this is that information does not get lost or end up in the wrong hands. In this microlearning you will learn why classifying information is important for your organization.

After the training you will be able to answer the following questions:

- Why is it important to correctly classify information?
- What are the most common classification types?
- What are the risks of losing certain classified information?
- How do you act when people ask for sensitive information?



DATA PRIVACY

LEARN

Introduction in GDPR (12 min)

The General Data Protection Regulation, or GDPR, has been in force since 25 May 2018. Since then, everyone is permitted to appeal to organizations regarding the compliance of this new European privacy legislation. In this training, you learn to discuss the main guidelines of the GDPR and the correct way of protecting, processing, and storing personal data.

After the training, you will be able to answer the following questions:

- What is the GDPR?
- What is personal data?
- What does the processing of personal data entail?
- Why is good protection of personal data important?
- What are the basic rules of the GDPR?
- What rights do data subjects have?
- What are the tasks and responsibilities of processing?
- What should you do to protect personal data?

ANCHOR

Privacy in practice (4 min)

Working with information is an important part of an organization. By correctly classifying information, you indicate which protection level is necessary. Everyone then knows which levels of confidentiality, integrity and availability they must apply when they are working with the information. The purpose of this is that information does not get lost or end up in the wrong hands. This awareness video explains why it is important to correctly classify every bit of information.

After the awareness video you will be able to answer the following questions:

- Why is it important to correctly classify information?
- What are the most common classification types?
- What are the dangers of losing information of a certain classification type?
- What do you have to do if people ask for information?

BUREAU VERITAS

PHISHING

LEARN

Phishing (11 min)

In this training, you will learn how to recognize and report a phishing attack. Every day, criminals attempt to steal sensitive information by using social engineering and other forms of deception. So make sure you are aware when someone is trying to mislead you. This training teaches you to pay extra attention to links and to what information you share. This way you protect yourself and your organization against phishers.

After the training you will be able to answer the following questions:

- What is phishing?
- How do phishers work and how do I recognize them?
- How do you avoid becoming a victim of phishing?

PRACTICE

Phishing (3 min)

Phishing is one of the biggest cybercrime threats at this moment. There are many forms of social engineering, but phishing is by far the most well-known and successful one. The idea is simple: after you have clicked on a link or opened an attachment, the cybercriminal has access to your information. This awareness video teaches you how you can recognize suspicious emails, what the dangers are and what you have to do if things go wrong.

After the awareness video you will be able to answer the following questions:

- What are phishing criminals looking for?
- How do you recognize a phishing email?
- What do you do if you do not trust a link or attachment?

ANCHOR

Know with whom you are dealing (1 min)

Social engineers pretend to be someone else. They do this via email, during telephone conversations or even face-to-face. But how do you find out with whom you are dealing? How do you prevent yourself from becoming a victim of social engineering? If you recognize a social engineer, you prevent yourself from giving up sensitive information. In a few minutes this microlearning shows you how you can figure out with whom you are dealing and teaches you how you handle suspicious situations.

After the training you will be able to answer the following questions:

- How do people with malicious intent get sensitive information?
- How do you ensure that you only share information with the right people?

MALWARE

LEARN

Malware (6 min)

Malware is short for ‘malicious software’. It is a collective name for different types of malicious software. Ransomware is a well-known type of malware. Malware can cause lots of damage to an organization. For example, personal information can be stolen or sensitive information can become public. This training ensures that you are aware of the dangers of the different types of malware. You learn to recognize malware and prevent infections.

After the training you will be able to answer the following questions:

- What is malware?
- What forms of malware exist?
- What does malware do?
- How can you recognize malware?
- How can you prevent malware?

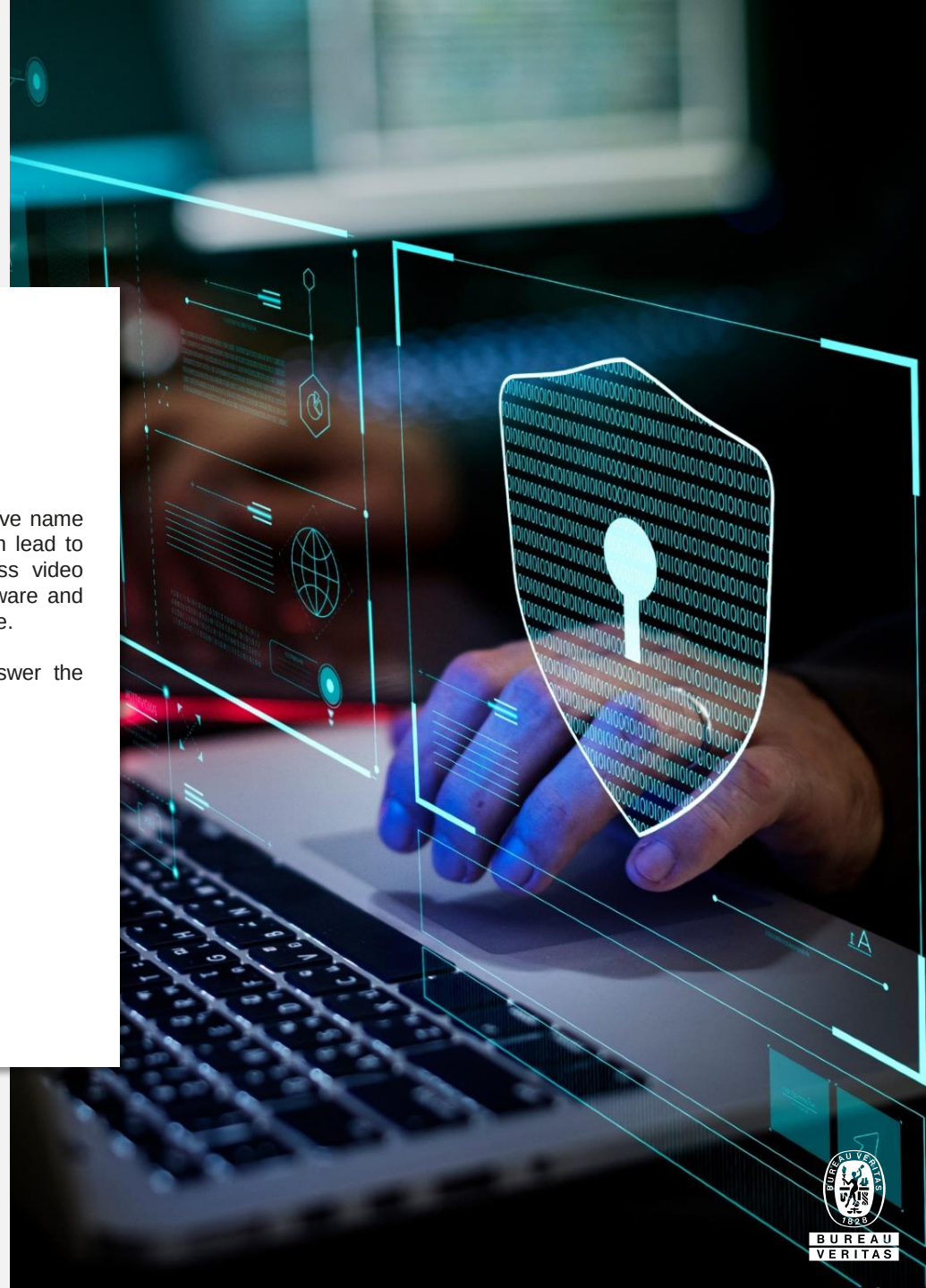
PRACTICE

Malware (4 min)

Malware stands for malicious software. It is a collective name for several types of malicious software. Malware can lead to serious damage in an organization. This awareness video teaches you by which signs you can recognize malware and what you need to do when you think you have malware.

After the awareness video you will be able to answer the following questions:

- What is malware?
- What does malware do?
- What are the signs of malware?



MOBILE DEVICES

LEARN

Mobile devices (5 min)

What do you have stored on your smartphone, laptop or tablet? It will not only be your own personal information. Maybe you have also saved company-sensitive information. This can have serious consequences if it ends up in the wrong hands. Many of us have never taken into account that this can happen, and also do not know what to do in this situation. In this training, you will learn how you can prevent the loss of your equipment and how you can work securely with it.

After the training you will be able to answer the following questions:

- In which ways is mobile devices used?
- What are the risks of using mobile devices?
- How can you limit these risks?
- What to do in case of an incident?

PRACTICE

Bring your own device (4 min)

If employees can use their own mobile equipment for business purposes, your organization also takes advantages of that. For example through lower service and hardware costs. Additionally, employees often have phones, tablets and laptops that are smarter, better and faster than the company equipment. This awareness video teaches you how you can use your own equipment for your work, what the dangers of doing that are and how you handle incidents.

After the awareness video you will be able to answer the following questions:

- How can you use your own devices for business purposes?
- What are the dangers of working with your own devices?
- How can you beat these dangers?
- What to do in case of a security incident?

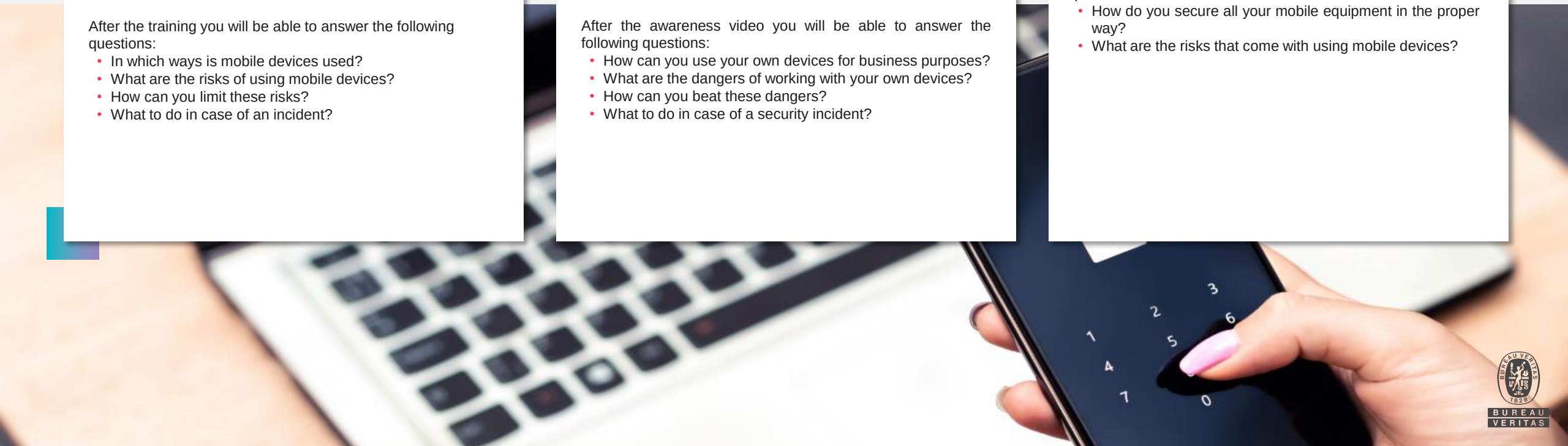
ANCHOR

Secure your mobile devices (3 min)

Mobile devices are always within reach. They have many advantages, but some of these advantages come with certain risks. If you are aware of these risks, you also know how to protect yourself against them. This microlearning explains why securing mobile equipment is important.

After the training you will be able to answer the following questions:

- How do you secure all your mobile equipment in the proper way?
- What are the risks that come with using mobile devices?



THE NEW WAY OF WORKING

LEARN

The new way of working (8 min)

The new way of working means that you can work any time and everywhere: at home, in public or at the flex spot wherever you want. But this way of flexible working is not without its information security risks. This training explains how you can take advantage of the advantages of the new way of working in an optimal and secure way.

After the training you will be able to answer the following questions:
- What is the new way of working?
- How do you work securely from home, in public or at flex spots?

PRACTICE

Social Media & working in clouds (4 min)

Social media enables you to reach a huge audience, but it is also a source of identity theft. Cloud services are very accessible, but with some cloud services the service provider has the same access rights to your information as yourself. To prevent this from having nasty consequences for you and your organization, you will learn in this awareness video about the risks of using social media and the cloud.

After the awareness video you will be able to answer the following questions:
- What kind of information is safe to share on social media and what kind is not?
- What are the risks of sharing information via a cloud service?
- How can you prevent incidents?

Working in public places (4 min)

Flexible working gets increasingly popular. More and more employees have the opportunity to from home, at the office, on the train or in a public space. But working in public does come with different security risks. In less than 2 minutes this awareness video teaches you how you optimally take advantage of working in public without being at risk of losing sensitive or confidential information.

After the awareness video you will be able to answer the following questions:
- What do you take into account when working in public?
- What do you pay attention to when using social media?

ANCHOR

Internet of Things (IoT) (7 min)

There are more and more 'smart' devices that form a network via the internet, such as smartwatches and external hard disks. Many of these devices are not properly secured. Hacked or infected 'smart' devices are a threat to company devices. It is often unclear which person within the organization is responsible for securing these 'smart' devices. In this micro-learning you learn how you, as an employee, can work as safely as possible with IoT devices.

After the training you will be able to answer the following questions:
- What is the IoT?
- How do IoT devices infect company equipment?
- What are the risks of the IoT?
- How do you deal with the weak spots of the IoT?

Work securely outside the office (3 min)

Working outside the office is different from working at the office. Outside the office you are working with mobile devices and you do not have a naturally secure internet connection. In about 3 minutes this microlearning teaches you how you can work optimally outside the office, without any risks of information security incidents.

After the training you will be able to answer the following questions: • How do you work securely with sensitive company information?
- What do you do with devices when you are not using them?
- How do you securely handle mobile devices?
- What do you do with documents containing sensitive information that are no longer necessary?
- How do you print in a secure way?
- How do you send sensitive information in a secure way?

BUREAU VERITAS

SOCIAL ENGINEERING

LEARN

Social Engineering (7 min)

Executives and managers play a crucial role in information security. In this introduction training, you not only learn why cybersecurity is important and how you handle cyber risks, but also get practical tips to protect the organization against cyber threats. After completing this training you can create a plan yourself, with which you can start working right away.

After the training you will be able to answer the following questions:

- What is cybersecurity?
- Why is cybersecurity important?
- Which cyberattacks are directly aimed at executives and the management?
- How important is cybersecurity for your organization?
- Which measures does your organization need?
- How do you work on cybersecurity within your organization?
- What do you do in case of an incident?

PRACTICE

Social Engineering (4 min)

Social engineering is a technique where someone tries to steal confidential information by manipulating the 'victim'. You are working with lots of information that is attractive to other people. It is therefore important that you can recognize the operating methods of social engineers. For example, always be careful with the information you are discussing in public. If you discuss sensitive information in public, other people can also hear this. That could have nasty consequences.

After the awareness video you will be able to answer the following questions:

- What is the target of social engineers?
- What do you have to pay attention to when you are having a business conversation in public?
- What do you have to do when a strangers asks for information?

RISK MANAGEMENT

LEARN

Risk management (10 min)

In this training, you will learn what risk management is, which risks you might encounter and what your role in this is. The training was developed for (project) managers, but other employees can also get the training so that they are better able to handle the risks. You discover what the role of the risk manager is within the organization, you learn how to map risks by way of a self-audit and you learn when to approach the risk manager for advice or support.

After the training you will be able to answer the following questions:

- What is the purpose of risk management?
- What is the role of the risk manager?
- What is a risk? • How do you map risks?
- What are the consequences of risks?
- Which management measures can you take?
- When do you approach the risk manager for advice or support?

PRACTICE

Access control (4 min)

This video shows why access control is important for the protection of information. The use of an access pass enhances the security of a building because only people with a pass have direct access. It also provides insights into who is present in the building. In case of calamities, that is important information to have. Therefore, always immediately report the loss of a pass to the department or person responsible.

After the awareness video you will be able to answer the following questions:

- What should you do with your access badge?
- How do you deal with visitors?

BUREAU VERITAS

OPERATIONAL TECHNOLOGY SECURITY

LEARN

Dilemma's in OT Security (25 min)

Cyber risks are unavoidable these days. Hackers do not take a day off and they would love to see their attack appear in the news. Of course, we do not want them to damage our services. Therefore, you are key in securing the systems and the premises. You are going to experience several dilemmas in an OT environment. Which choice do you make: convenience or security?

After 15-20 minutes, you can answer the following questions:

- Why is OT security important?
- How do you deal with physical security risks?
- How do you deal with cybersecurity risks?
- What do you do in case of an incident?

SHAPING A WORLD OF TRUST

Bureau Veritas is a Business to Business to Society company, contributing to transforming the world we live in. A world leader in testing, inspection and certification, we help clients across all industries address challenges in quality, health & safety, environmental protection and social responsibility.

For more information,
contact Bureau Veritas:

Le Triangle de l'Arche
8 cours du Triangle
CS 90096
92937 Paris La Défense Cedex
FRANCE
bureauveritas.com

BUREAU VERITAS

Shaping a World of Trust