

infosecure

know what you show

**E-Learning programs
for sustained behavior change**

Overview e-learning modules



you never know who's peeping

Secure your future growth by unlocking our security awareness library with more than 30 current risk topics

Introduction programs

Present the most important information security topics in an accessible and familiar way with our information programs. In only 20-30 minutes, your employees learn the correct way of working. An introduction program is the perfect start to an awareness-raising campaign.

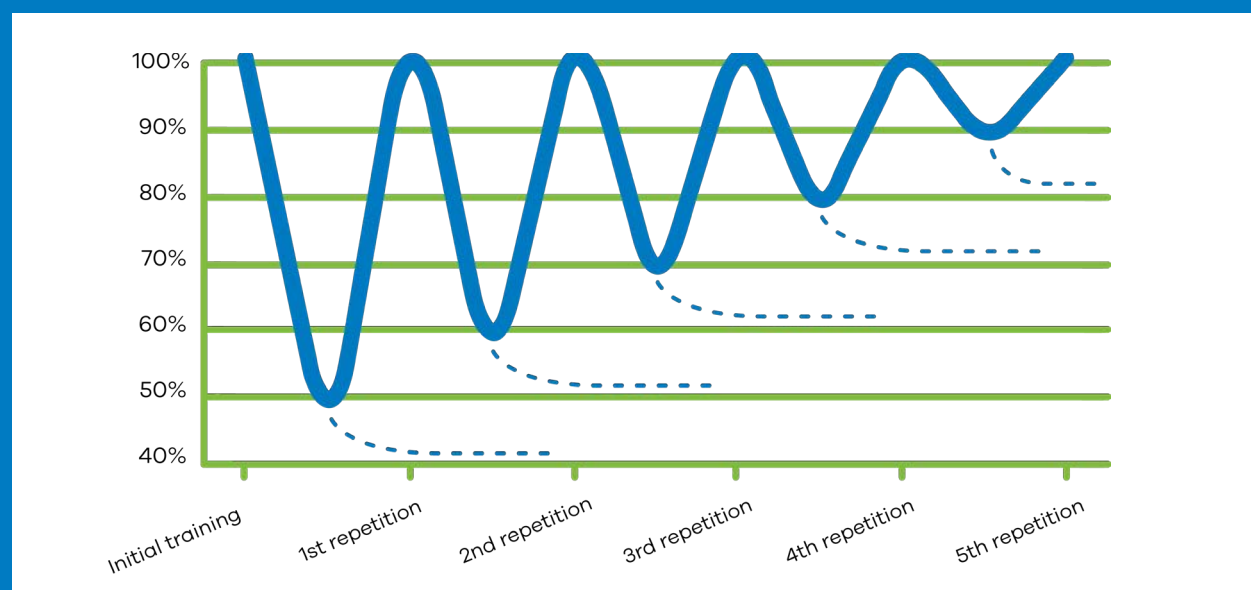
- > Information security introduction program
- > Security by design
- > Cybersecurity for executives

In depth e-learning

In-depth e-learning modules delve deeper into topics that relate closely to day-to-day activities. The modules last 10-15 minutes and start off with a general introduction. The modules contain immersive videos, interactive content, test questions, and a conclusion. In-depth modules can also be used for specific target groups.

- > NEW: Ransomware
- > Phishing
- > Social engineering
- > Mobile devices
- > Cybersecurity
- > Working in the cloud
- > Information classification
- > Malware
- > Risk management
- > Physical security
- > General Data Protection Regulation (GDPR)

Forgetting curve



Repeating knowledge regularly helps you to retain information. Our microlearnings and security flashes refresh knowledge in 1 to 5 minutes.

Microlearning

- NEW: Data protection and privacy
- Data protection and privacy- under lock and key
- Shadow IT
- Working from home - There's no place like home
- Use of passwords
- Work securely outside the office
- Secure your mobile devices
- Know with whom you are dealing
- Reporting information security incidents
- How is information classified?
- Ransomware
- Internet of Things
- Privacy in practice

Security flashes

- Bring your own device
- Clear desk, screen & office
- Phishing
- Reporting security incidents
- Strong passwords
- Working in public spaces
- Social engineering
- Access control
- Social media and working in the cloud
- Information classification

Baseline tests

Our baseline tests provide a useful picture of what employees know at a certain point in time, as well as gaps in their knowledge.

- Cybersecurity
- Phishing
- Risk management
- General Data Protection Regulation (GDPR)
- Malware
- Physical security



Introduction program

Information security - In the front line

Keeping information secure is easier said than done. The time has passed when taking technical measures alone was sufficient to keep security threats at bay. Nowadays, the most important weapon against cybersecurity threats are the people who work with the information every day. They form the first line of defense. .

What do you do when strange things are happening? Are you able to keep information secure? Meet Maya. She can use some help.

After 15-20 minutes participants will be able to answer the following questions:

- How do you keep information in your workplace safe?
- What are the risks of the digital world and how do you protect yourself against that?
- What do you do in case of an incident?

Security by design - Functionality vs security

When designing a new application, developing new software, or managing a system, it's important that it functions properly. Usability and user experience are a priority. But what is a user-friendly security measure worth if hackers can bypass it? A robust infrastructure needs a good balance between functionality and security.

This training offers the foundation you need to find that balance. A security researcher gives you advice and tangible tips for designing, developing, and managing applications, software, and systems in a safe and secure way.



After 15-20 minutes participants will be able to answer the following questions:

- Which different kinds of security assessments can you use?
- Why is patch management important?
- What is Coordinated Vulnerability Disclosure and how does it help with IT management?
- Why is the OWASP valuable?
- How does the principle of 'defense in depth' help when developing a secure infrastructure?

Cybersecurity for executives

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 cyberrisks, but also get practical tips to protect the organization against cyberthreats. After completing this training you can create a plan yourself with which you can start working right away.

After 15-20 minutes participants 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?



In-depth e-learning

NEW: Ransomware - Layer by layer

Ransomware attacks are the object of every security officer's nightmare. We might think we know better than victims of these attacks. However, when that ONE phishing mail goes unnoticed and that ONE administrator account has a weak password, the price you pay is just too high. Not only in terms of money, but also the price of dealing with a siege of the entire computer network.

Peprico & partners are doing everything they can to minimize risks and have started an investigation. Let's join them in their quest to find answers!

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

- How do hackers gain access to our computers and network?
- What are warning signs of a possible ransomware attack?
- Which preventive measures can you take to protect against ransomware attacks?

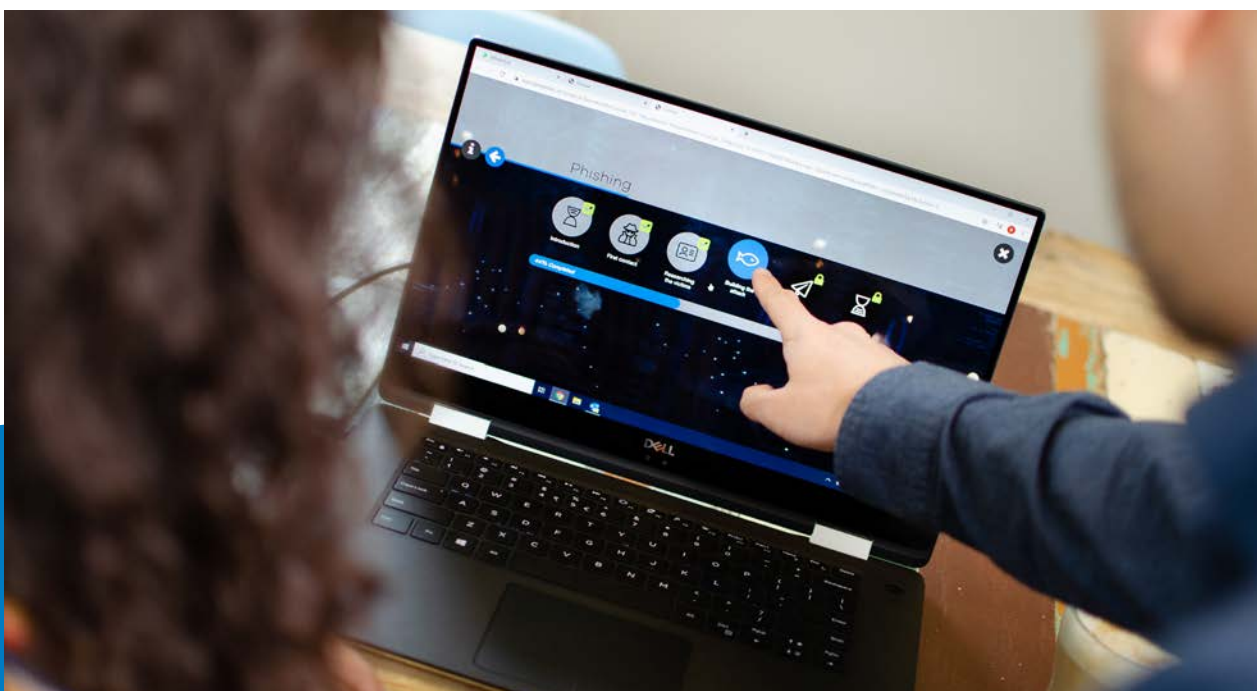
Phishing - The flip side of phishing

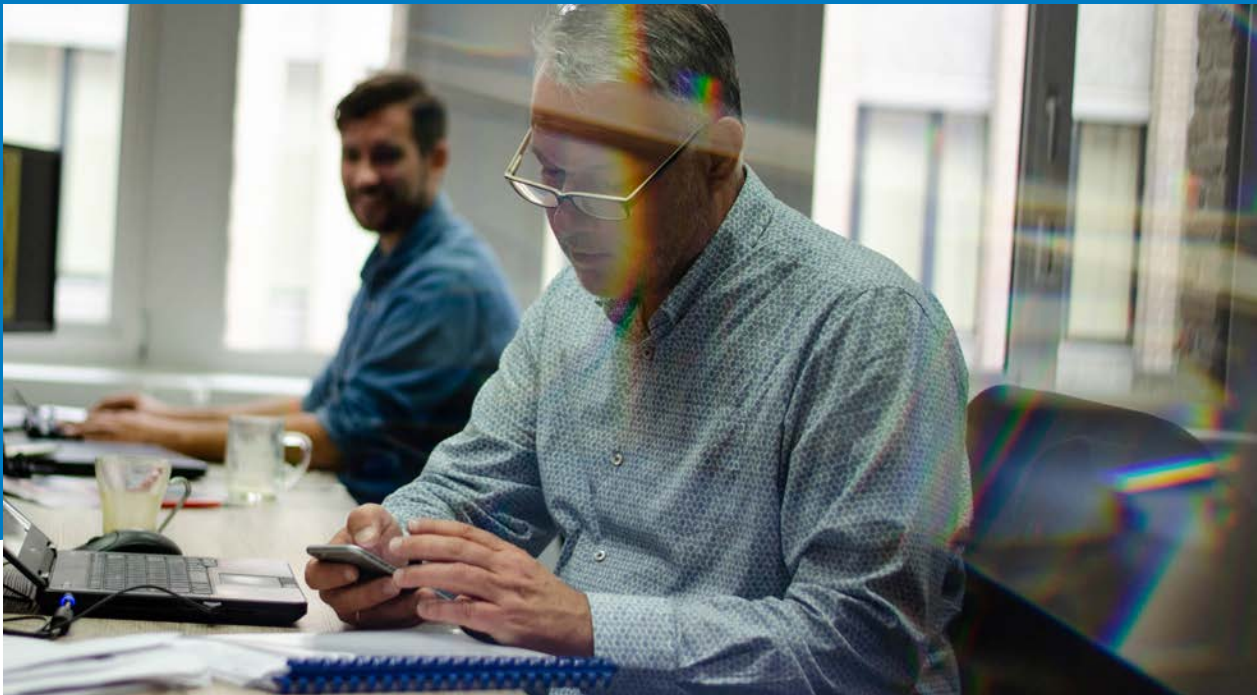
Up until a couple of years ago, phishing mails were easy to recognize. They were filled with language errors, copied and pasted logos and subject titles in CAPSLOCK. Nowadays phishing mails are way more realistic and harder to recognize. You don't have to be a programmer to send a phishing mail, so more and more scammers try their luck. Profits can reach up to millions of euros. How do you create a phishing mail? What does a phisher keep in mind when preparing an attack?

Are you ready to look at the flip side of phishing?

After 15-20 minutes participants will be able to answer the following questions:

- What are the signs of phishing and how can you recognize them?
- How do phishers find out information about their victims?
- How does phishing via social media differ from phishing via email?
- How can you protect yourself against the dangers of phishing?





Social engineering - The social dilemma

The time when cybercriminals focused solely on computer hacking is behind us. They've found a way that is just as effective, or maybe even more so: human hacking! Manipulating and influencing people can lead to great profits. They send phishing messages, try to persuade us via the phone, or, for the real risk takers, physically enter an office to steal sensitive information. You play a key role in protecting the organization's information from these types of attacks. Start the story to find out how.

After 15-20 minutes participants will be able to answer the following questions:

- What is 'social engineering'?
- What tactics do social engineers use?
- How do you recognize an act of social engineering?
- How should you deal with suspicious situations?

Mobile devices - All eyes on you

It's your first day at your new job, but as soon as you meet your new team there is a big problem. Information about a new project has leaked and can be found all over the internet. Luckily, it's not disastrous yet; the information isn't sensitive, but the leak could develop to a serious leak with major consequences. It's up to you to investigate and find out where it's going wrong.

After 15-20 minutes participants will be able to answer the following questions:

- What are mobile devices and why is it important to protect them?
- What are the dangers of apps and how do you protect your mobile devices against them?
- How do you protect your mobile devices against the dangers of public Wi-Fi networks?
- How can you keep information on your mobile devices safe, even when they are stolen or lost?

Cybersecurity

In this training you will learn about the meaning, the risks and the importance of cybersecurity. You follow Rosa during her workday and see how she protects the security of digital information. You will learn about measures that you can take during your everyday work to protect the security of digital information.

After 15-20 minutes participants will be able to answer the following questions:

- What is cybersecurity?
- How do you recognize a phishing email and how do you respond to this?
- How do you protect your login information and accounts?
- How do you securely save information?
- What is the Internet of Things and how do you handle it securely?
- How do you securely use the internet?
- How do you prevent becoming a victim of social engineering?

Working in the cloud

With the cloud you have access to information at any time and any place. It offers huge possibilities, but also comes with risks. If you know how to work securely in the cloud, you can optimally use the advantages. In this training you learn everything you should know to work securely in the cloud.

After 15-20 minutes participants will be able to answer the following questions:

- What is working in the cloud?
- What is a public cloud service and what are the advantages and disadvantages?
- What is a private cloud service and what are the advantages and disadvantages?
- How do you work securely in the cloud?

Information classification

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 15-20 minutes participants 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?



Malware

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 15-20 minutes participants 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?

Risk management

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 15-20 minutes participants will be able to answer the following questions:

- 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?

Physical security

Physical security protects the people and properties of an organization, but also information. Besides technical security, information also needs physical security. The most important threats against which physical security protects an organization, are intentional threats from people. Examples are theft and accidental access. In this training you will learn which measures an organization can take to ensure physical security and what your role is in this.

After 15-20 minutes participants will be able to answer the following questions:

- What is physical security?
- Why is physical security important?
- How do you contribute to physical security yourself?

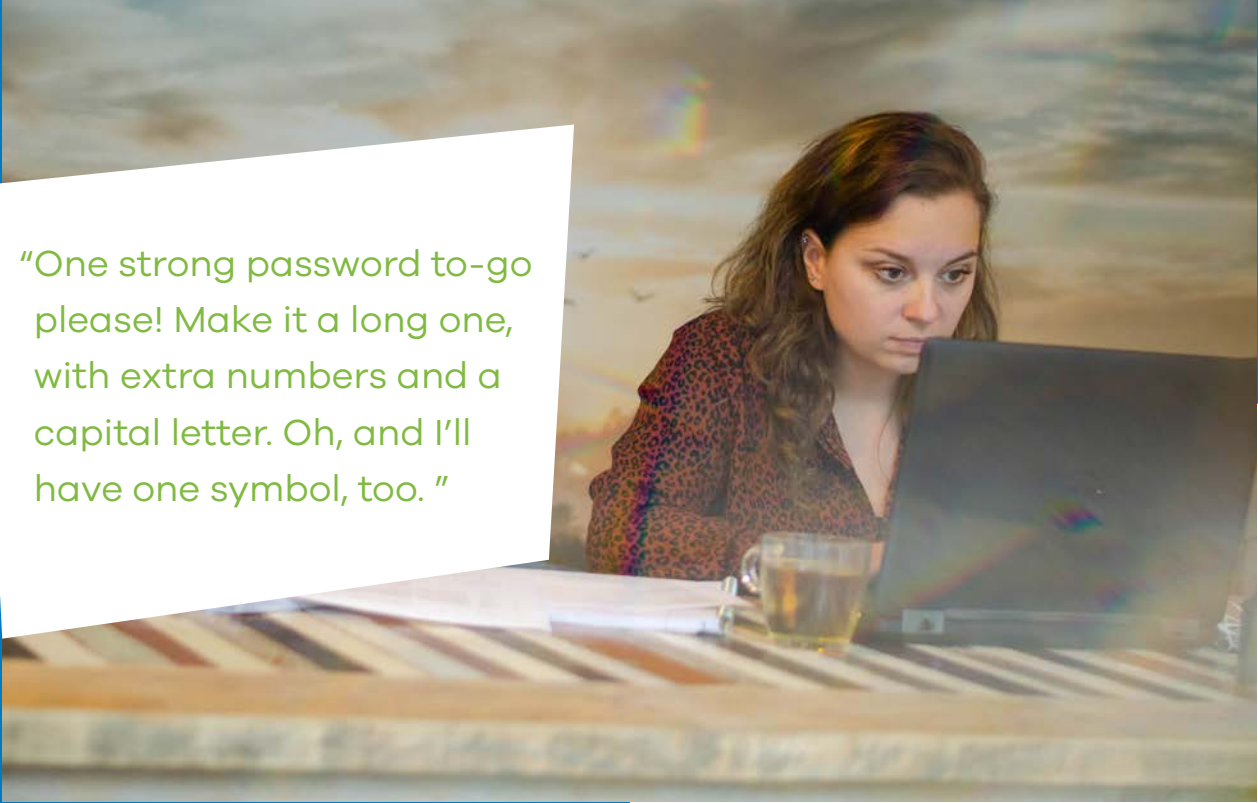
General data protection regulation (GDPR)

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 15-20 minutes participants 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?





"One strong password to-go please! Make it a long one, with extra numbers and a capital letter. Oh, and I'll have one symbol, too. "

Microlearning

NEW: Data protection and privacy

Do you value your privacy? It's good to know that your privacy is safeguarded by several laws. But how does this translate to your daily work? In this microlearning you help Oliver and Eveline to make the right choices.

After 5 minutes, you will be able to answer questions such as:

- What is (sensitive) personal data?
- How do you keep personal data safe?
- What can you do when something goes wrong and you cause a data breach?

Use of passwords - P@ssw0rd1

You probably know how to make a strong password. But there's more. Handle your passwords properly, and your information will be safer still. So sit down for a moment, get a cup of coffee and discover how to use passwords in a smart way.

After 5 minutes participants will be able to answer questions such as:

- Which accounts do you protect first?
- How do you make a strong password?
- What is two factor authentication?
- How do you check if your passwords have been leaked?
- What are the benefits of a password manager?

Working from home - There's no place like home

When you're at home, you're not only in charge of the coffee but also of office security. This means that it's your responsibility to make sure you work in a safe way. In this microlearning, you will follow our colleague, Mina, around who will show you the security-basics of working from home.

After 5 minutes, participants will be able to answer questions such as:

- How can you ensure that you don't share more information than intended during an online meeting?
- What do you do with business documents and devices after your workday is done?

Shadow IT - Step out of the shadow

Convenience can cost more than you might think! Using a free file-sharing application to quickly share a file or using your personal device to finish an important document might seem like an easy and convenient option. However, there's a darker side to the use of these solutions that you might not be aware of...

After 5 minutes, participants will be able to answer questions such as:

- What is "Shadow IT"?
- What are the risks of using "Shadow IT"?





Secure your mobile devices

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 5 minutes participants will be able to answer questions such as:

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

Know with whom you are dealing

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 5 minutes participants will be able to answer questions such as:

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

Report information security incidents

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 5 minutes participants will be able to answer questions such as:

- 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?

How is information classified?

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 5 minutes participants will be able to answer questions such as:

- 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?

Ransomware

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 5 minutes participants will be able to answer questions such as:

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





Internet of things (IoT)

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 5 minutes participants will be able to answer questions such as:

- 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?

Privacy in practice

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. This microlearning teaches you, on the basis of practical situations, how to apply the GDPR in practice.

After 5 minutes participants will be able to answer questions such as:

- What is (special) personal data?
- Why is personal data protection important?
- How do you deal with privacy in practice?

Security flashes

Bring your own device

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 this 2-3 minutes awareness video participants 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?

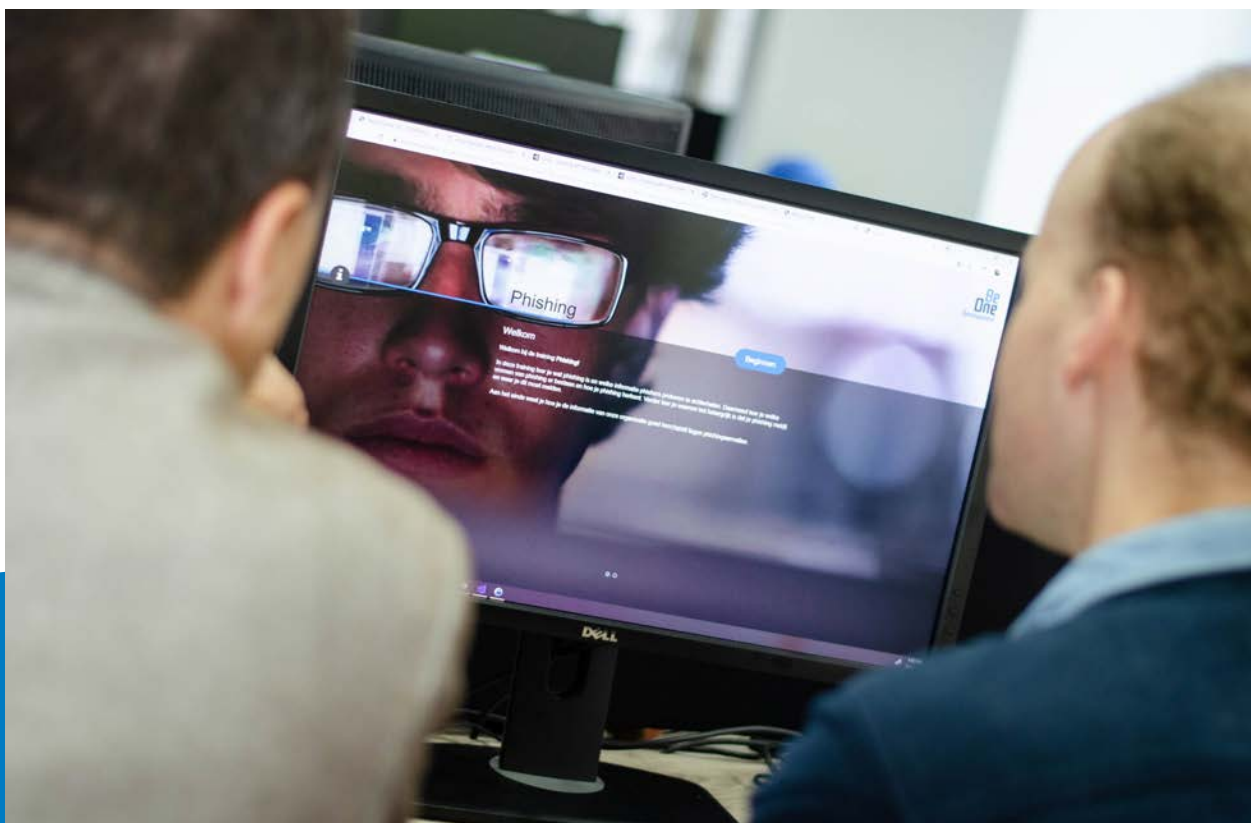
Clear desk, screen & office

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 2-3 minutes awareness video participants 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?





Phishing

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 this 2-3 minutes awareness video participants 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?

Report security incidents

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 this 2-3 minutes awareness video participants 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?

Strong passwords

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 2-3 minutes awareness video participants 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?

Working in public places

Flexible working gets increasingly popular. More and more employees have the opportunity to work wherever and whenever they want: 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 this 2-3 minutes awareness video participants 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?





Social engineering

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 this 2-3 minutes awareness video participants 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 stranger asks for information?

Access control

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 this 2-3 minutes awareness video participants will be able to answer the following questions:

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

Social media & working in the cloud

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 this 2-3 minutes awareness video participants 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?

Information classification

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 this 2-3 minutes awareness video participants 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?



Malware

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 this 2-3 minutes awareness video participants will be able to answer the following questions:

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

Data protection and privacy – Under lock and key

Do you value your privacy? It's good to know that your privacy is safeguarded by several laws. But how does this translate to your daily work? In this microlearning you help Oliver and Eveline to make the right choices.

After 5 minutes, you will be able to answer questions such as:

- What is (sensitive) personal data?
- How do you keep personal data safe?
- What can you do when something goes wrong and you cause a data breach?

Baseline test

Baseline test information security

The baseline measurement shows the current knowledge level within the organization. This is not a test. So we do not expect that you complete the baseline measurement without making any mistakes. The results clarify which topics require more attention. This is how we adjust the training sessions and information to what is necessary right now. Via the training sessions we offer more information about the topics.

The baseline test deals with the following topics:

- General Data Protection Regulation (GDPR)
- Cyber security
- Physical security
- Malware
- Phishing
- Risk management

Convinced or do you want us to tell you more? For all further details about our products and services, our rates and manner of working, please visit:

<https://www.infosecure.com/contact>

Engaging references

Infosecure's e-learning programs have proven their success in hundreds of multinationals, medium-sized enterprises, governmental organizations, and institutions across the globe. All of these organizations are now more secure after their employees learned how to keep cyber risks at bay using our programs.

- > Antoni van Leeuwenhoek hospital
- > Bank of Cyprus
- > Bertelsmann
- > Boskalis
- > Municipality of Maastricht
- > Philips

Interested to learn how Infosecure can help to focus your employees?

For any questions about our e-learning programs, please get in touch. We'd be happy to give you a demonstration.

For more information, visit
www.infosecure.com



infosecure

Olympia 2L, 1213 NT Hilversum, The Netherlands
Phone: +31 (0)85 30 397 10
www.infosecure.com