Check the 78 potential threats that undermine your IT security

Checklist for Cybersecurity training

eloomi

Make your employees a part of your cyber defence

Employees are the cause of over 50% of all IT security breaches*

We spend a lot of resources on protecting our systems from malicious actors. But what's the point if our own employees let the hackers straight in?

Multiple studies show that the majority of IT security breaches are caused by employees' lack of knowledge and proper caution. 70%* of employees would click on a link in a phishing email if they haven't been trained in how to spot them, and it only takes one click to expose your company data and leave your systems vulnerable to attacks.

At the end of the day, employee-behaviour is the number one risk to your IT security. Your colleagues should be a part of your cyber defence but all-too-often they're precisely the opposite.

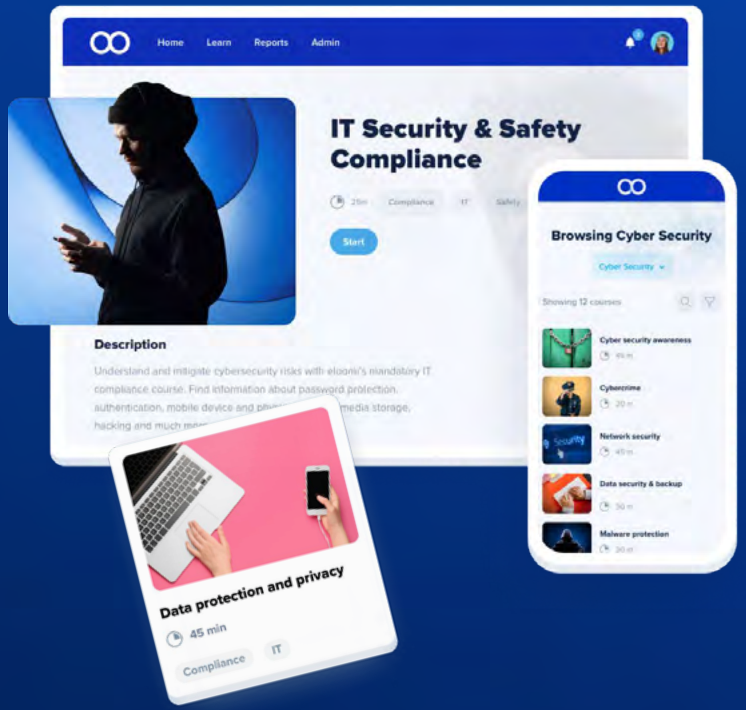
acker attack - what do we do?
aud
IT security
Securing your IT equipment
Compliance
IT
Using a company mobile phon
Compliance
IT security
Passwords
IT security
Passwords

* Source: SHRM (Society for Human Resource Management), FireEye

with eloomi

Train your employees in cyber defence

- Are your employees properly prepared to combat the growing threat of cyber attacks?
- Do you have up-to-date records of what training has been delivered out and by who?
- Are new employees onboarded with cybersecurity training, or has it been forgotten?
- New threats are always arising, do you keep your training up to date to stay prepared?



Description

Understand and mitigate cybersecurity risks with eloomi's mandatory IT compliance course. Find information about password protection, authentication, mobile device and phy media storage, hacking and much mo

✓ eloomi is the easy and flexible e-learning solution your employees can use on the go.

✓ Access engaging courses to keep employees certified and compliant with full reporting on progress and completion.

✓ All this makes your job as the IT security watchdog infinitely easier.

The IT Director’s cybersecurity checklist

(and action plan)

We’ve made it easy and practical to assess your IT security training. Use our list of e-learning courses as your comprehensive checklist.

☒ **Cross off the checkbox** when you’re sure your employees are fully prepared.

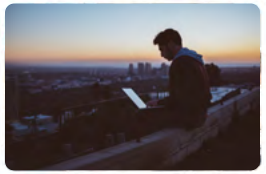
□ **Leave the checkbox empty** if you aren’t 100% sure your employees are up to date.

For each empty checkbox, you have a vulnerability in your IT security - as well as a recommended course to secure your compliance training.

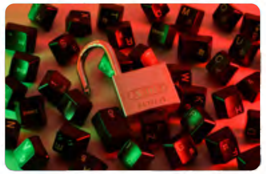
Understand and mitigate cybersecurity risks with eloomi's mandatory IT compliance course.

Is your cybersecurity at risk?

Go through the checklist and see how you measure up.



1 We can work from anywhere – with total security. We think.



2 Bad passwords

3 Not in line with GDPR & laws for handling sensitive information

4 Failing to recognize phishing and scams

5 Lacking key knowledge of IT security

6 Underestimating physical IT security risks

7 Unable to identify malware and hacking attempts

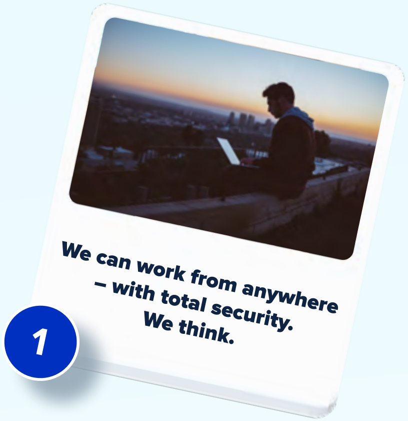
✓ Test results

1

We can work from anywhere – with total security. We think.

We work everywhere. Across different devices and wifi-connections. Do you have full confidence in your employees' conduct? Cross off the checkbox for each area where you feel your employees fully understand and follow the necessary IT security guidance.

- □ **Free WiFi.** It's easy for hackers to monitor what other people are doing when they're connected to the same free WiFi.
- □ **Home Wi-Fi.** If you're working from home, make sure your home WiFi is secure and encrypted.
- □ **Juice Jacking.** Always charge your devices using your own charger and cable.
- □ **Home Wi-Fi (Vacation version)** Make sure you're using WiFi securely, even while working abroad or from on holiday.
- □ **Physical media.** It's easier to steal physical data than hacking into databases or guessing passwords.
- □ **Removable media.** There is a risk to using removable media. Make sure to encrypt your documents in case your flash drive gets lost or stolen.
- □ **Social media sharing.** Be careful what you share on social media.
- □ **Unknown Networks.** Hackers can set up a Wi-Fi access point and if you connect to it much of your communication can be monitored or even manipulated.
- □ **Valuables in car.** If you are trusted with confidential information on electronic media or printouts, leaving them in an unsupervised car is not safe.
- □ **VPN. Working from home.** A VPN connection creates a virtual tunnel between your laptop or smart device and your office servers.
- □ **Work email handling.** Work email should be used for work purposes only — and not only because of work-life balance.
- □ **Working from home. Insider threat.** "Insider threat" usually refers to employees who leak data, but data can also be leaked by friends or family.
- □ **Working from home – Unattended computer.** Keep your computer safe and locked when working from home.



2

Bad passwords

Are your employees on the ball when it comes to password protection? The list below will show you where you might have cracks in your security, which need to be corrected with IT training.

□ **Password handling.** It's hard to juggle multiple passwords, but writing them down and storing them by your computer is what hackers are hoping for.

□ **Multi factor authentication.** Hackers have been after passwords since the dawn of the Internet and they are surprisingly adept at stealing them and even guessing them.

□ **Passphrases.** Forget complex passwords ... oh wait, we already did!

□ **Password manager.** We will always need passwords but remembering them can be difficult.

□ **Passwords.** To create a strong password, it's best to use a combination of lower case, upper case letters, symbols and numbers.

□ **Same passwords.** Managing multiple passwords can be hard, but using the same password for every account is a huge security risk.

□ **Password sharing.** Some things are simply not meant to be shared.

3 Not in line with GDPR & laws for handling sensitive information

Do your employees know the rules when it comes to handling personal data? Or are you at risk of employees failing to give due caution, and compromising your organization? It's better to prevent than cure. Which areas on the list below should your employees brush up on?

□ **Auto-fill.** Sometimes confidential information leaks out because email senders are in a hurry or distracted and select the wrong recipient.

□ **Clean desk.** Our desks are not a safe place for confidential documents.

□ **Company credit cards.** Don't let cybercriminals charge their shopping spree to your organization's credit card.

□ **Data leaks.** A data leak is the intentional or unintentional release of secure or private/ confidential information to an untrusted environment.

□ **Doublecheck before you trust.** We should always consider the possibility that an email account could have been hacked and that messages and requests from co-workers or business partners could be fake.

□ **Dumpster diving.** A lot of valuable information could be gathered by going through your workplace's trash.

□ **GDPR – Personal information.** If a customer asks you to forget about them, you must comply.

□ **Handling confidential material.** Your personal email and online storage are usually not a safe as your work email.

□ **Keep it safe.** Can your clients trust you with their information? Do you guard it like it is your own?

□ **Network printer.** The main risk factor when using a networked printer is that if you select the wrong printer, confidential material can reach unauthorized eyes, inside or outside the workplace.

□ **Online PDF makers.** Don't choose convenience over security.

□ **Printouts.** When printing, remember to dispose of your documents properly.

□ **Sharing information.** Be extra careful who you deliver confidential information to. Make sure the recipient has the authority to access the information.

□ **Social engineering.** Don't share confidential information with people who do not have authorization. Not even your best friends.

□ **Unnecessary data.** Read up on the privacy laws you need to follow in your day to day work. Failure to comply might result in fines for your workplace.

Not in line with GDPR & laws for handling sensitive information
3

4 Failing to recognize phishing and scams

Cybercriminals have a full toolkit of methods designed to identify and hit the weak points of your organization. Can your employees spot a phishing email, or are you vulnerable to data leaks and attacks? Here's an overview of the knowledge your employees need to prevent hacker attacks.

- □ **CEO scam.** Always double check unusual requests from your boss, especially regarding financial transfers.
- □ **Check account number.** Fraudsters might try to sneak a bogus invoice into your Accounting Department. You should always double-check new account numbers.
- □ **Correct links.** Hover over links in emails before you click on them to make sure they'll lead you to the right place.
- □ **Doublecheck before you trust.** Be aware that there is always a possibility that someone has been "listening in" on your email conversations.
- □ **Extortion emails.** Cybercriminals sometimes rely on our insecurities to extort hush money or phish for more information.
- □ **Malicious attachments.** All mail is not necessarily good mail. Don't open attachments or links from unknown senders.
- □ **Online shopping risk.** The biggest risk when shopping online is not that you could simply lose your money.
- □ **Phishing.** Every day, 8 million people open a fraudulent phishing email and that is how most cyber-attacks start.
- □ **Phishing urgency.** A tone of urgency in an email is one of the key indicators of a phishing email.
- □ **Romance scams.** Social engineering - Watch out for red flags in new digital relationships. Preying on people's loneliness is a common tactic of scammers.
- □ **Spear phishing.** Knowing about someone's interests and hobbies is valuable and helps hackers create spear phishing emails specifically designed for that person.
- □ **Spear phishing II.** Be mindful of what you share on social media. Cybercriminals can use our interests and hobbies to create targeted phishing emails that look legitimate.

- □ **Vishing.** When a person calls you on the phone and uses a false reason or claim to trick you into handing over personal or sensitive information, such as your social security number or credit card information, that's called Vishing.

5 Lacking key knowledge of IT security

Do your employees run a tight operation, preventing hackers from finding their way inside your system? Are they aware of potential dangers, and up to date with the latest threats? Use the checklist below to find the answers, and discover potential vulnerabilities that you can use to guide your IT security training.

□ **Chain mail.** It's highly unlikely that chain-mail contains relevant information. If you forward it you're just wasting everyone's time.

□ **HTTPS connections.** A website address starting with HTTPS is encrypted and much safer than a website address starting with HTTP.

□ **Misinformation.** Check the source - All that glitters is not gold, nor is everything on the internet the truth. Be careful what you believe and share online.

□ **Phonelocking.** Documents, memos, emails and contacts can be stolen if you leave your phone unlocked.

□ **Popups.** Do you know the proper way to shut down pop-ups?

□ **Security Awareness Training.** When we know about the dangers all around us we can take precautions and try to navigate our world more safely.

□ **Security culture.** Creating and maintaining a good security culture in the workplace is something that all businesses should strive for.

□ **Software installs.** Make your IT technician's job easier and don't install software on your work computer without permission.

□ **Think before you post.** Think twice before you post or comment on your social media sites. How will this reflect on you or your workplace?

□ **Think twice.** Inter-office emails can be fun, but we still need to remember proper email etiquette.

□ **Unattended computer.** Leaving your computer unlocked and unattended can cause serious problems if someone else has access to it.

□ **Update your software.** Patching your software whenever you get notified of an available update could sae you a lot of trouble and time in the long run.

□ **Zoom bombing.** With great new technologies come great new threats.

6

Underestimating physical IT security risks

Could a stranger stroll into your office party and get access to confidential material? Do you have a policy for visitors in the building? The physical side of IT security is important, and all-too-often forgotten. Check your potential blindspots below. Is there an area where your employees need a refresher?

- □ **Privacy screens.** Using a privacy screen is a very affordable way to dramatically increase your security when working outside the office.
- □ **Let the right one in (Halloween special).** Make sure that only employees have access to the workplace, both during and outside working hours.
- □ **Shoulder surfing.** Cyber criminals don't just guess or hack your password. Sometimes they simply watch you type it in.
- □ **Stakeout.** Always be aware of your surroundings.
- □ **Tailgating.** Hackers rely on the kindness of strangers to gain access to restricted areas.
- □ **Tailgating II.** All workplaces should have strong policies and procedures in place when it comes to letting strangers into restricted areas.

7

Unable to identify malware and hacking attempts

Spyware, malware, ransomware. Most people have heard of them, but how do you predict how a hacker will try to enter your system, and what do you do to prevent it? Check to see if your employees are fully up to date on these topics.

- □ **Conference risk.** Beware of free portable memory drives and charging banks.
- □ **Keylogger.** Check your computer ports regularly for unknown devices.
- □ **Microsoft risk.** Do not enable editing on Office documents unless you're absolutely sure.
- □ **Mobile listening.** Beware! Malware could be installed on your smartphone which turns on your camera and microphone to listen in on your conversations.
- □ **Personal USB drives**. Your home computer is not as well protected as your work computer.
- □ **Ransomware.** Ransomware is a virus or malware that encrypts the data on your computer or your whole network.
- □ **Ransomware attack.** Accepting software updates or downloads from a website is risky business.
- □ **Spreading viruses.** If you install unapproved software on your work computer, the whole office network could become infected with a virus.
- □ **Spyware.** How does spyware get onto your computer? Here's one way.
- □ **Spyware in attachments.** When it comes to distributing viruses, spyware or other malware, there is no method more popular among hackers than attachments.
- □ **USB key drop.** What should you do when you find a USB flash drive? Whatever you do, don't plug it into your computer.

Results

0	78
Completely covered	Potential vulnerabiltiies

Did you have a lot of holes in your IT security?

There's a lot that your employees need to know and stay up to date on if you want to be fully secure.

✓ Luckily, it's easy to get things going in the right direction with eloomi - plus you've already identified your action plan.

✓ We'd love to connect you with world-class content – book a demo here!

eloomi offers flexible e-learning that your employees will love

Making your life easier!

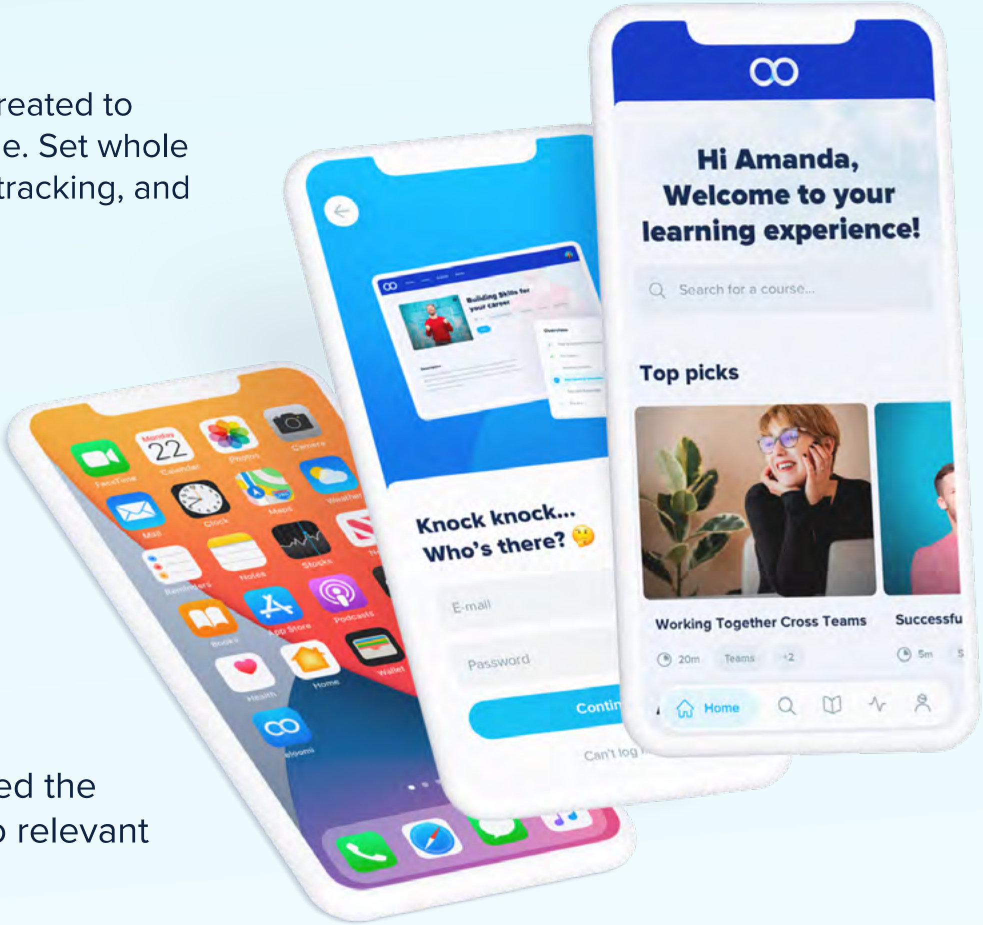
Hiring and onboarding new employees places ever-increasing demands on your workplace's ability to communicate. And carrying out training is no exception. That's why you need to choose a platform with care.

eloomi is an award-winning and innovative e-learning platform, created to streamline your onboarding and compliance training from day one. Set whole new standards of working with skills development, engagement tracking, and completion reports.

✓ **Global learning content**
Developed in collaboration with leading IT security experts

✓ **Flexible training**
Give your employees the freedom to take classes wherever and whenever suits them best

✓ **Reporting and automation**
Keep an eye on whether your employees have completed the necessary training and ensure automatic enrollment into relevant courses



Hi Amanda, Welcome to your learning experience!

Knock knock... Who's there?

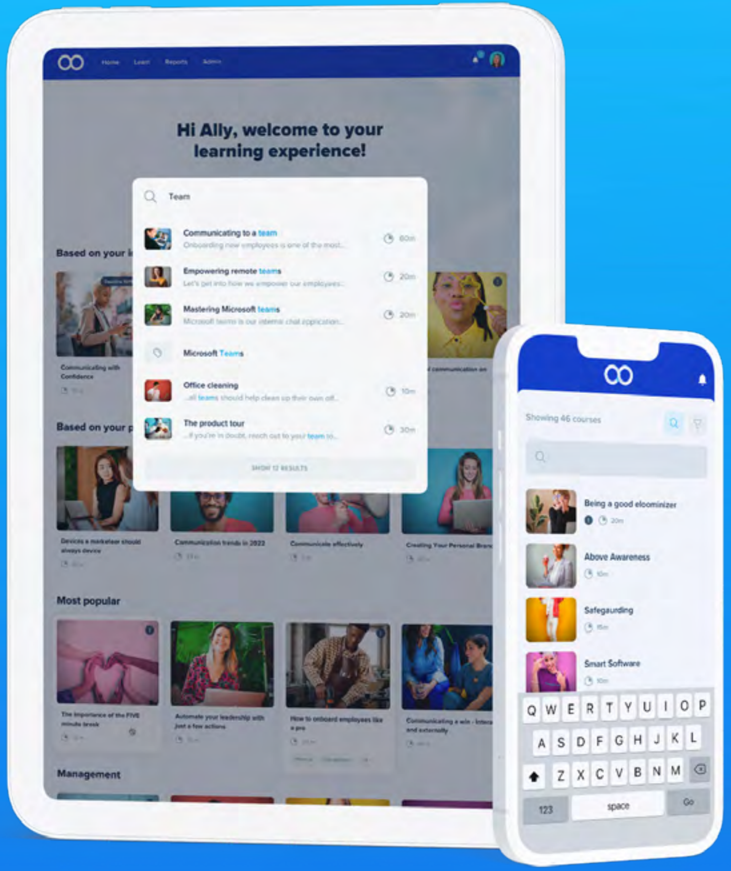
Sharpen your defences against cyber attacks – start now!

✓ With eloomi, you eliminate the weak points in your IT security and lower the risk of being hit by a successful cyber attack.

✓ Raise your employees' awareness and understanding of IT security's importance and create a strong and consistent IT security culture.

Book a demo →

Start today


Home
Learn
Reports
Admin
Hi Ally, welcome to your learning experience!
Team
Communicating to a team
Empowering remote teams
Mastering Microsoft teams
Microsoft Teams
Office cleaning
The product tour
Based on your i
Based on your p
Communicating with Confidence
Devices a marketeer should always device
Communication trends in 2022
Communicate effectively
Creating Your Personal Bran
Most popular
The importance of the FIVE minute break
Automate your leadership with just a few actions
How to onboard employees like a pro
Communicating a win - intern and externally
Management
Showing 46 courses
Being a good eloominizer
Above Awareness
Safegaurding
Smart Software
Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M
123
space
Go