**go**Deep

Cyber
Security
Awareness
Training

@phishgodeep

# 1 in 10 employees will click on the link in a phishing email letting the hackers in.
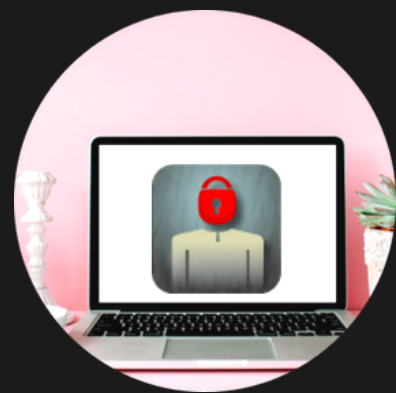
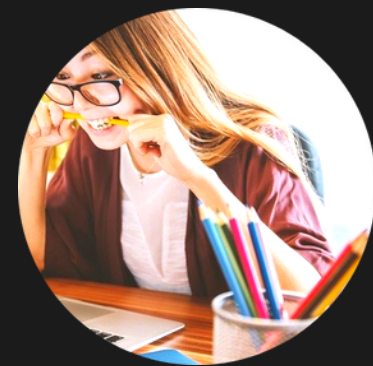**goDeep**

## CYBER SECURITY AWARENESS TRAINING

When it comes to cyber security, companies can become bogged down in the details. This inertia leaves a company vulnerable with untrained employees exposing your organisation to serious cyber attack. It's not a matter of if, but when your employee's lack of knowledge will be exploited by hackers to access your system. Hackers will cause damage to your business reputation and finances.

goDeep Cyber Security Training teaches all employees their vital role in keeping business safe, empowering staff to avoid attacks with automated phishing simulations and breach monitoring.
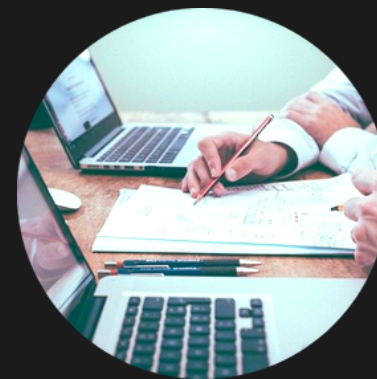
## PLATFORM FEATURES

ONLINE TRAINING

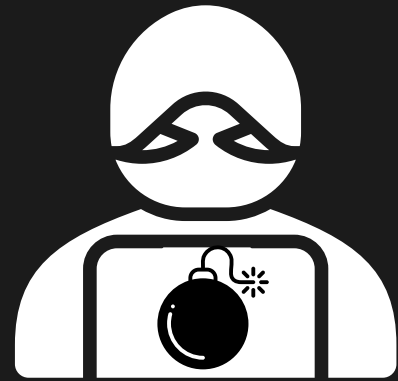SIMULATED PHISHING

REPORTS COMPLIANCE

BREACH MONITORING

# Why do companies need to introduce Cyber Security Awareness Training?

Hackers will damage a business. If there is a financial loss, the chances of ever recouping the funds is minimal. Even with law enforcement involved the criminals will never be caught.

With so many employees working at home, IT departments are being pushed to the limit.
36% of companies reported a cyber security incident with a remote employee. Training is essential to keep a business cyber secure.
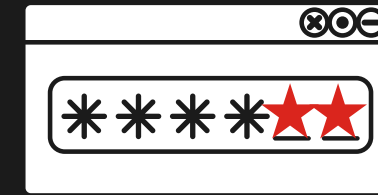
66% of people reuse passwords. Even people who admit they know it is bad practice take the risk. goDeep alerts users and their employer if staff passwords and credentials are exposed in a publicized data breach on the dark net.

10% of small businesses that suffer a cyber breach will shutdown permanantly after the attack. Training is essential so all employees understand how important their role is in cyber security.
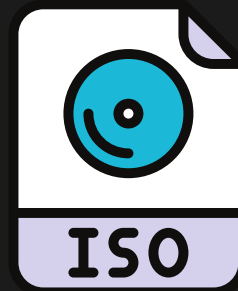
Implementing cyber security training is an essential part of GDPR compliance and ISO27001 certification. Companies seeking cyber security insurance would also benefit having goDeep.

IBM estimates the average cyber data breach costs a company 3.9 million US Dollars. This loss can be prevented by teaching employees to be a virtual human firewall.
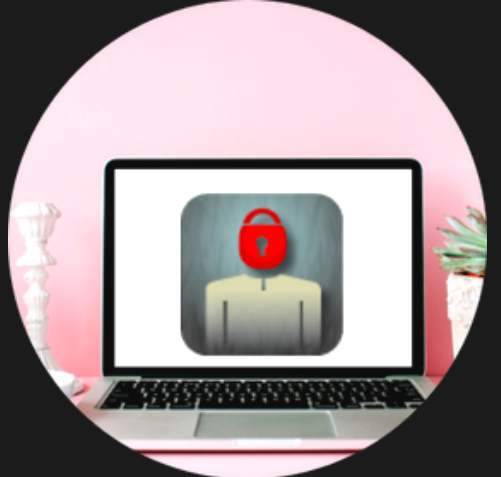
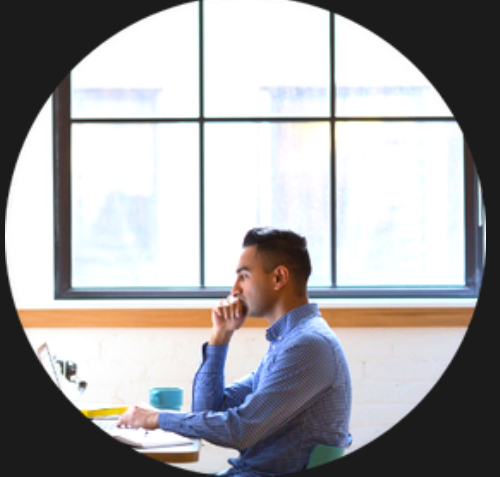In 2021, Cybercrime cost business 1 trillion euro

Employees need training to act as the first line of defense against cybercrime

# The goDeep platform offers business the chance to roll out cyber security to the whole company, covering all bases and making employees a human firewall.

## TRAIN
goDeep Online training teaches cyber security awareness

## EDUCATE
Teach employees to be the company first line of defence

## TEST
Continuously test employee cyber savvy in a safe environment
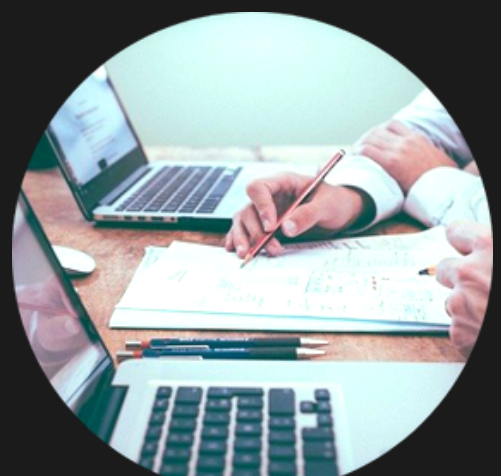
## DOCUMENT
Record employee training progress & phishing response

## TRACK
Know your organization is on guard and who is vulnerable

## REPORT
Use goDeep to report on employee awareness for ISO27001 and GDPR
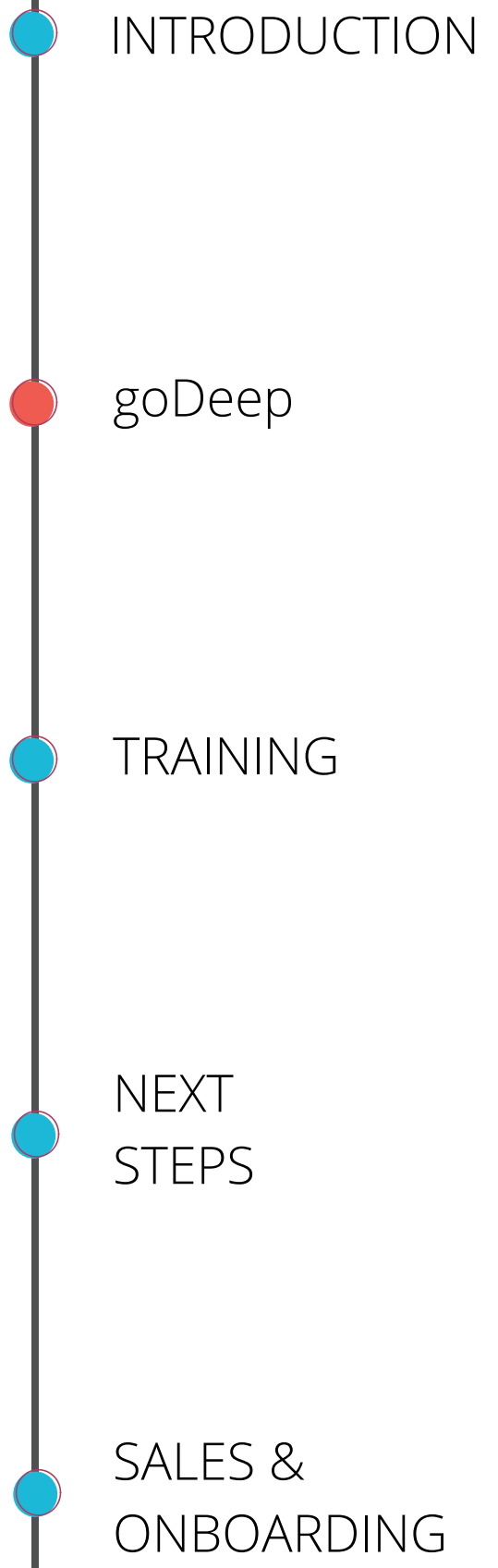
goDeep's combination of approachable training and automated continuous phishing simulation teaches employees to be on guard. goDeep teaches staff to spot suspicious emails, be cyber aware and keep your business safe.

goDeep's easy to understand online training makes cyber security accessible to the whole team

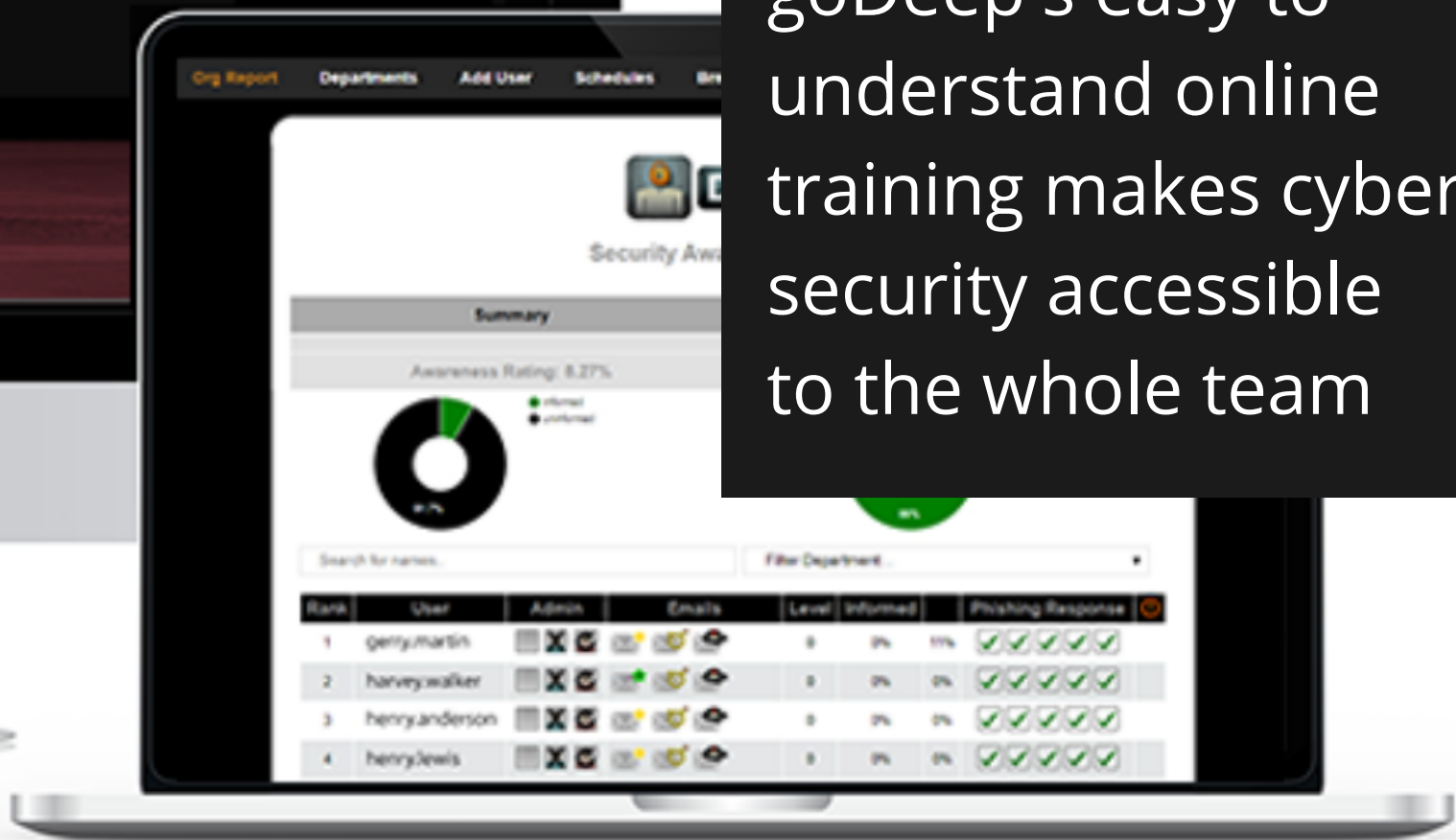# goDeep offers comprehensive online Cyber Security Awareness Training

## MODULES INCLUDE

### INTRODUCTION
As our digital footprint continues to expand goDeep reviews the types of data we keep online. goDeep explains the threats that come with hackers accessing your data and gives tips how to protect it.

### PASSWORDS
People create more and more passwords every day to protect their online data. Here we demonstrate simple ways to improve password security and what to do if your password is compromised.

### SECURITY IN PUBLIC SPACES
We often use insecure methods to access the internet without considering the implications to our personal and professional data. goDeep provides advice on how to remain secure in public places.

### PHISHING
Phishing is now the primary attack vector that bad actors employ to gain access to business computers and data. goDeep shows how to spot common techniques used, explaining why hackers are so successful.

### INFORMATION SECURITY AT HOME
With employees working at home surrounded by an increasing number of household devices connected to the internet, cyber criminals sense opportunity. goDeep shows how to secure your digital footprint at home.

### SOCIAL ENGINEERING
It is widely accepted that people are the weakest link when it comes to information security breaches. goDeep shows common human hacking techniques that are used by attackers to trick employees to let them in.

### GENERAL DATA PROTECTION REGULATION
The General Data Protection Regulation protects our privacy by enforcing stringent requirements for those who process personal data. goDeep shows your team how to comply with this regulation

INTRODUCTION

goDeep

TRAINING

NEXT STEPS

SALES & ONBOARDING

The phishing problem facing business is enourmous. Research has shown the number of fake emails sent each day far outnumbers legitimate emails composed and sent.

Even the most robust firewall and spam filter is still vulnerable to phishing or fake email attack.

85% of organizations report experiencing phishing or malware attacks. goDeep helps protect your business by teaching employees to be on guard against fake phishing emails.

In addition to our cyber training, goDeep continuously tests employees. goDeep's automated phishing simulations are conducted in a safe environment, testing and reinforcing the training and keeping staff on their toes.

goDeep's reporting features allow companies to track employee progress and performance, highlighting who may be vulnerable to cyber attack.

When it comes to cyber security, prevention is key. An extensive cyber attack can cause irreparable damage and needs to be avoided. goDeep helps your customers stay safe.
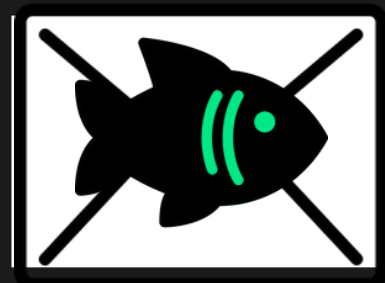
Phishing emails can be incredibly sophisticated, and well researched. Often the email will appear to be from a friend or colleague.
A successful phishing campaign can cause untold damage to a company's reputation and finances.
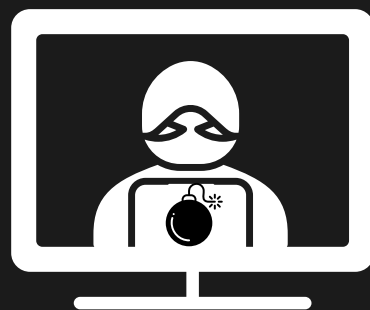
Untrained Employees are the vulnerability hackers need to find their way into a company. Teaching employees to be cyber aware empowers employees to keep the business safe.

goDeep targets staff with risk free phishing simulations helping them to recognize the evolving techniques used by fraudsters. Phishing attacks are used to steal data and commit crime against your clients or their business connections.

Are you interested in learning more about goDeep?

# What next?

- Check out our website, dctsecurity.com for more information
- Book a demo of goDeep with the goDeep team
- Sign up for the extended goDeep free trial
- We show you the ropes with free Virtual Onboarding Sessions
- Follow our social media accounts for cyber security content and news.

The goDeep team would be delighted to speak with you regarding the goDeep program and how goDeep can help employees keep the company safe by being cyber aware.

Contact us to get started:   info@dctsecurity.com

# We are here to help

From Firewalls to email trying to get your head around IT Security can be daunting. That is where DCT Security come in to help. Our experienced team can audit your systems, train your team and test your networks. By spotting vulnerabilities and recommending important changes DCT Security helps to keep your business  safe, secure and on guard against potential attacks.

Our product goDeep was designed to make cyber security accessible to everyone. We worked to make the goDeep platform easy to use and run.

We offer our customers free set up and can conduct online training with your team on how to use and administer goDeep.  We also offer first class customer support with our customer care team.

Our goDeep team are always here to help        info@dctsecurity.com

# Thank you!

Please don't hesitate to reach out if you have questions or queries about our fantastic cyber security platform, goDeep.

We are happy to show potential customers how the goDeep platform works with an online demo where we can discuss how goDeep can help to make your employees into a virtual human firewall keeping your business safe.

email: info@dctsecurity.com