Content Library

Transforming habits one click at a time

Security Awareness Modules

GoldPhish combines high-quality, engaging and relevant training modules, interactive eLearning, animation videos, real-world scenarios and regular assessments.

Interactive eLearning, Animation Video, Knowledge Assessment

Cyber Threats

Approx. 10 minutes

Cyber crime is on the rise and everyone is a potential target. This module introduces users to the different types of criminals who frequent and use the Internet and explores why they, their family, or their company might be a valuable target for criminals.

Interactive eLearning, Animation Video, Knowledge Assessment

Safe Web Browsing

Approx. 10 minutes

The Internet is a minefield of cyber threats and potential traps. This training module teaches users how to avoid common pitfalls and dangers associated with web browsing. Users will also learn how to recognise secure encrypted websites.

Interactive eLearning, Animation Video, Knowledge Assessment

Malware

Approx. 10 minutes

New types of malware are developed and deployed by criminals every day to attack devices and end users. This module provides brief but comprehensive training about malicious software, a significant and rising threat across all markets.

Interactive eLearning, Animation Video, Knowledge Assessment

Passwords

Approx. 10 minutes

A password is your account's first line of defence, but it's also vulnerable to cyber attacks. This training module covers topics such as password strength, password diversity, along with the best password security practices for keeping users' accounts secure.

Security Awareness Modules

GoldPhish combines high-quality, engaging and relevant training modules, interactive eLearning, animation videos, real-world scenarios and regular assessments.

Interactive eLearning, Animation Video, Knowledge Assessment

Social Engineering

Approx. 10 minutes

Social engineering is the use of deception to manipulate individuals into divulging information that may be used for fraudulent purposes. This module explains the dangers associated with smishing, vishing, and in-person attacks.

Interactive eLearning, Animation Video, Knowledge Assessment

Phishing

Approx. 10 minutes

A majority of cyber-intrusion attempts begin with phishing emails. These social engineering attacks are delivered via malicious links, file attachments, and login forms. This training module helps show the warning signs to look out for and what to do in the event of a phishing attack.

Interactive eLearning, Animation Video, Knowledge Assessment

Business Email Compromise

Approx. 10 minutes

BEC scams occur when attackers impersonate company stakeholders and trick your employees into transferring money or sharing confidential information. Users will learn how to recognise these scams and learn basic best practices to protect against them.

Interactive eLearning, Animation Video, Knowledge Assessment

Mobile Device Security

Approx. 10 minutes

Criminals often target our mobile devices as a means for penetrating our accounts and information. This training module will teach users the importance of physical and technical safeguards for their mobile devices.

Security Awareness Modules

GoldPhish combines high-quality, engaging and relevant training modules, interactive eLearning, animation videos, real-world scenarios and regular assessments.

Interactive eLearning, Animation Video, Knowledge Assessment

Social Media Safety

Approx. 10 minutes

Cyber criminals use social media platforms to find their victims and the data needed to launch attacks. This training module will teach users how to protect themselves, their families, and their employers while using social networks.

Interactive eLearning, Animation Video, Knowledge Assessment

Insider Threat

Approx. 10 minutes

Often an organisation's biggest threat to their data and security is right under their nose. This interactive training module examines the potential for a company's own employees, either intentionally or unintentionally, to inflict damage on the organisation.

Interactive eLearning, Animation Video, Knowledge Assessment

Physical Security

Approx. 10 minutes

Securing the workplace and restricting physical access to devices and IT infrastructure is essential to securing data and online systems. This module will explain why physical security is important and how users can improve physical security in the workplace.

Interactive eLearning, Animation Video, Knowledge Assessment

Cyber Safe Travel

Approx. 10 minutes

Users often let down their guard when travelling or working remotely and convenience often trumps secure practices. This training module will teach users how to secure devices and keep sensitive information secure when out of the office and on the road.

Security Awareness Modules

GoldPhish combines high-quality, engaging and relevant training modules, interactive eLearning, animation videos, real-world scenarios and regular assessments.

Interactive eLearning, Animation Video, Knowledge Assessment

Cyber Safety at Home

Approx. 10 minutes

Cyber criminals don't discriminate and will often target personal devices and accounts as easy targets. This training module will teach users how to secure family devices and networks as well as keep sensitive information secure at home.

Interactive eLearning, Animation Video, Knowledge Assessment

Information Security

Approx. 10 minutes

Protecting sensitive information is fundamental to preventing reputational damage, business loss and identity theft. Users will learn how to responsibly handle and protect personal and company confidential information.

Interactive eLearning, Animation Video, Knowledge Assessment

Incident Response

Approx. 8 minutes

It is inevitable that most people and organisations will fall victim to some form of cyber crime, and how you immediately respond to the incident can make all the difference. This module provides basic training about responding to a cyber incident.

Interactive eLearning, Animation Video, Knowledge Assessment

Executive Training

Approx. 30 minutes

This extended interactive module is designed to help company executives, senior managers and team leaders better understand information and cyber security threats to the business environment, and their potential impact on company success.

Compliance Modules

Short engaging content perfect for keeping all employees aware of data protection laws and the behaviour required for staying complaint.

GDPR

Approx. 10 minutes

Personal data is associated with significant risk if stolen and abused, therefore the General Data Protection Regulation (GDPR) was introduced to specify how personal data should be used and protected. This short awareness module introduces this data protection law, its requirements, and how it applies to you as an employee and consumer.

POPI Act

Approx. 10 minutes

Many companies hold extremely sensitive personal information on their customers and employees, obtained from various sources. Personal Data is associated with significant risk if stolen and abused, therefore the Protection of Personal Information Act (POPIA) was introduced in South Africa to specify how personal data should be used and protected.

HIPAA

Approx. 15 minutes

HIPAA training is one of the most important aspects of HIPAA compliance. HIPAA compliance training provides employees with a HIPAA introduction including how to recognise protected health information (PHI), proper uses and disclosures of PHI, how to keep PHI secure, and how to report a breach of PHI.

PCI DSS

Approx. 10 minutes

The PCI DSS is a set of policies and procedures intended to optimise the security of credit, debit, and cash card transactions, and protect cardholders against misuse of their personal information. This module unpacks this data protection standard, its requirements, and how it applies to you as an employee and consumer.

Micro-Modules

Each micro-module dives into a single security behaviour that users can embrace to become safer online, both at home and in the workplace.

Enable MFA

2 min.

Learn how to enable and maintain Multi-Factor Authentication for all accounts.

Strong, Unique Passwords

2 min.

Learn how to use strong and unique passwords across accounts.

Simplify with SSO

2 min.

Learn how to use Single Sign-On (SSO) for simplified and secure access.

Password Managers

2 min.

Learn how to use a password manager application.

Browser Password Saving

2 min.

Learn how to save passwords or passphrases into a browser.

Use Biometric Security

2 min.

Learn how to use biometrics for securing access to devices and accounts.

Micro-Modules

Each micro-module dives into a single security behaviour that users can embrace to become safer online, both at home and in the workplace.

Adopt Passkeys

2 min.

Learn how to use passkeys for securing access to accounts.

Avoid Breached Passwords

2 min.

Learn how to avoid using passwords compromised in data breaches.

Spot Deception

2 min.

Learn how to check emails and messages for signs of deception.

Dodge Phishing Emails

2 min.

Learn how to avoid interacting with potential phishing emails.

Hyperlink Caution

2 min.

Learn how to exercise caution with hyperlinks to prevent phishing.

Report Phishing

2 min.

Learn how to promptly report suspicious communications and phishing attempts.

Micro-Modules

Each micro-module dives into a single security behaviour that users can embrace to become safer online, both at home and in the workplace.

Update Regularly

2 min.

Learn how to regularly update and maintain software and operating systems.

No Rooting

2 min.

Learn how to ensure mobile devices are not rooted.

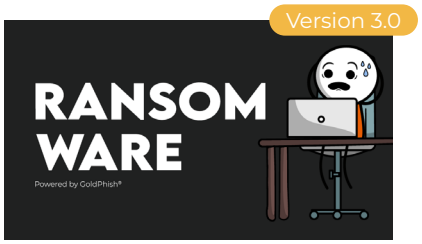
Install Antivirus

2 min.

Learn how to install and maintain antivirus and firewall protections on devices.

Video Content

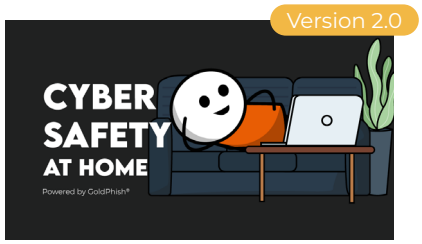
Engage learners in key cyber security subjects with short and entertaining animated videos.
Perfect for monthly reinforcement content.



Ransomware

2 min. 38 sec.

Ransomware is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. This short video introduces ransomware, discusses how it is delivered, and explains the effect of an infection. Users are provided with best practices for minimizing the threat of ransomware.



Cyber Safety At Home

3 min. 19 sec.

Cyber criminals don't discriminate and will often target personal devices and accounts as easy targets. This short video will teach users how to secure family devices and networks as well as keep sensitive information secure at home.

Clean Desk Policy

2 min. 13 sec.

Employees should be aware of best practices to prevent sensitive information from being viewed by unauthorised sources. This would include locking computers when unattended, keeping sensitive files in a locked cabinet when not in use, and being aware of your surroundings when working on sensitive data.

Physical Security

2 min. 16 sec.

Physical security is about protecting secure areas that require privileged access. Employees should understand the risks of propping open doors and their role in protecting secure areas. Terms such as piggybacking and tailgating are simply explained as well as knowing where to report such activities.

Video Content

Engage learners in key cyber security subjects with short and entertaining animated videos.
Perfect for monthly reinforcement content.

Protecting Business Information

2 min. 04 sec.

Protecting sensitive information is fundamental to preventing reputational damage, business loss and identity theft. In this short video users will learn how to responsibly handle and protect personal and company confidential information.

Identity Theft

2 min. 24 sec.

Identity theft is when fraudsters access enough info about someone to commit identity fraud. It impact their personal finances and their ability to obtain loans, credit cards or a mortgage until the matter is resolved. Employees need to understand how to keep personal information safe as well as the information of their peers, co-workers, and customers.

Phishing

3 min. 16 sec.

A majority of cyber-intrusion attempts begin with phishing emails. These social engineering attacks are delivered via malicious links, file attachments, and login forms. This short video helps show the warning signs to look out for and what to do in the event of a phishing attack.

Passwords

2 min. 30 sec.

A password is your account's first line of defence, but it is also vulnerable to cyber attacks. This short video covers topics such as: Password strength and password diversity along with the best password security tools and practices for keeping your account secure.

Video Content

Engage learners in key cyber security subjects with short and entertaining animated videos.
Perfect for monthly reinforcement content.

Business Email Compromise

2 min. 09 sec.

BEC scams occur when attackers impersonate company stakeholders and trick your employees into transferring money or sharing confidential information. Users will learn how to recognise these scams and learn basic best practices to protect against them.

Mobile Device Security

2 min. 51 sec.

Criminals often target our mobile devices as a means for penetrating our accounts and information. This training module will teach users the importance of physical and technical safeguards for their mobile devices, as well as ways to improve the security of their mobile communications and connections.

Intro to Cyber Security

4 min. 10 sec.

This short video introduces some general security concepts and to raise awareness about how to avoid online threats that might target you or our organisation. By identifying common online threats, understanding risk factors for each type of threat, and learning how to minimise the risk of an attack.

Social Engineering Scams

2 min. 26 sec.

Social engineering is the use of deception to manipulate individuals into divulging information that may be used for fraudulent purposes. This video explains the dangers associated with smishing, vishing, and in-person attacks. Users will learn how to keep themselves and their assets secure.

Video Content

Engage learners in key cyber security subjects with short and entertaining animated videos. Perfect for monthly reinforcement content.

Social Media Safety

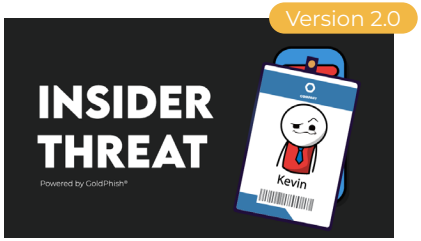
2 min. 07 sec.

Dive into our informative video, crafted to educate users on navigating social media with caution. Learn to safeguard your personal space, protect your family, and secure your employer's data against the crafty tactics of cyber criminals.

Safe Web Browsing

2 min. 34 sec.

The Internet is a minefield of cyber threats and potential traps. This short video teaches users how to avoid many of the common pitfalls and dangers associated with web browsing. They will learn how URLs are constructed, URL warning signs, and how to identify and avoid malicious links.



The Insider Threat

2 min. 25 sec.

Often an organisation's biggest threat to their data and security is right under their nose. This interactive training module examines the potential for a company's own employees, either intentionally or unintentionally, to inflict damage on the organisation.

THANK YOU!

Jess Massyn
Global Sales Director
jess@goldphish.com

Lesley Stone
Global Customer Success Manager
lesley@goldphish.com