# Phriendly Phishing

## Course Library

INNOVATION IN LEARNING

2021 SILVER WINNER

THE LEARNING AWARDS

**To add additional courses to your subscription, contact our team today**

support@phriendlyphishing.com
phriendlyphishing.com

# Subscriptions

All Phriendly Phishing Subscriptions come with the Phriendly Phishing dashboard, outlook S.C.A.M. reporter and varying levels of course access to meet your company's individual needs.

| | LITE | PLUS | PREMIUM |
|---|---|---|---|
| **Phishing Training / S.C.A.M. Series**<br>S.C.A.M. 101, 201, 301 & S.C.A.M. Family | ✓ | ✓ | ✓ |
| **Keep Secure Training**<br>Keep Secure & Keep Secure Mini | ✗ | ✓ | ✓ |
| **General Security Awareness Courses**<br>Covering topics including online security, workplace security, social media, remote working & more! | ✗ | ✗ | ✓ |

# Our Courses

## Included in Lite

### S.C.A.M. / Phishing Series (10-20 min each)

Our core phishing training series including:

1. S.C.A.M. 101 (gain knowledge)
2. S.C.A.M. 201 (apply knowledge)
3. S.C.A.M. 301 (create awareness & increase ability)
4. S.C.A.M. Family Edition (7 min)

## Included in Plus

### Keep Secure Series (10min each)

1. Security Foundations
2. Cyber-Attack Evolutions
3. Social Engineering
4. Online & Remote Threats
5. Internal Threats
6. KSec5 Framework / Making Intelligent, Ongoing Security Decisions

### Keep Secure Mini-Series (7 min each) N

1. Security Foundations
2. Social Engineering
3. 5 Rules to Keep Secure

## Included in Premium

### General Security Awareness (5 min each) N

1. An Introduction to Information Security
2. Bring Your Own Device (BYOD)
3. Business Email Compromise*
4. Cloud Security
5. Email Security
6. Handling Sensitive Information
7. Information Classification
8. Information Security at Work
9. Laptop Security
10. Mobile Phones and Tablets
11. Passwords and Passphrases
12. Personal Information
13. Protecting Credit Card Information
14. Protecting your Digital Identity
15. Safety Online
16. Scams and Social Engineering
17. Security Incidents
18. Security in the Workplace
19. Situational Awareness
20. Smishing*
21. Social Media
22. Vishing*
23. WiFi

### Government Guidelines (10-15 min each) N

1. Removable Media
2. Privileged Access Management
3. Secure by Design
4. Security Incident Response
5. Information Privacy

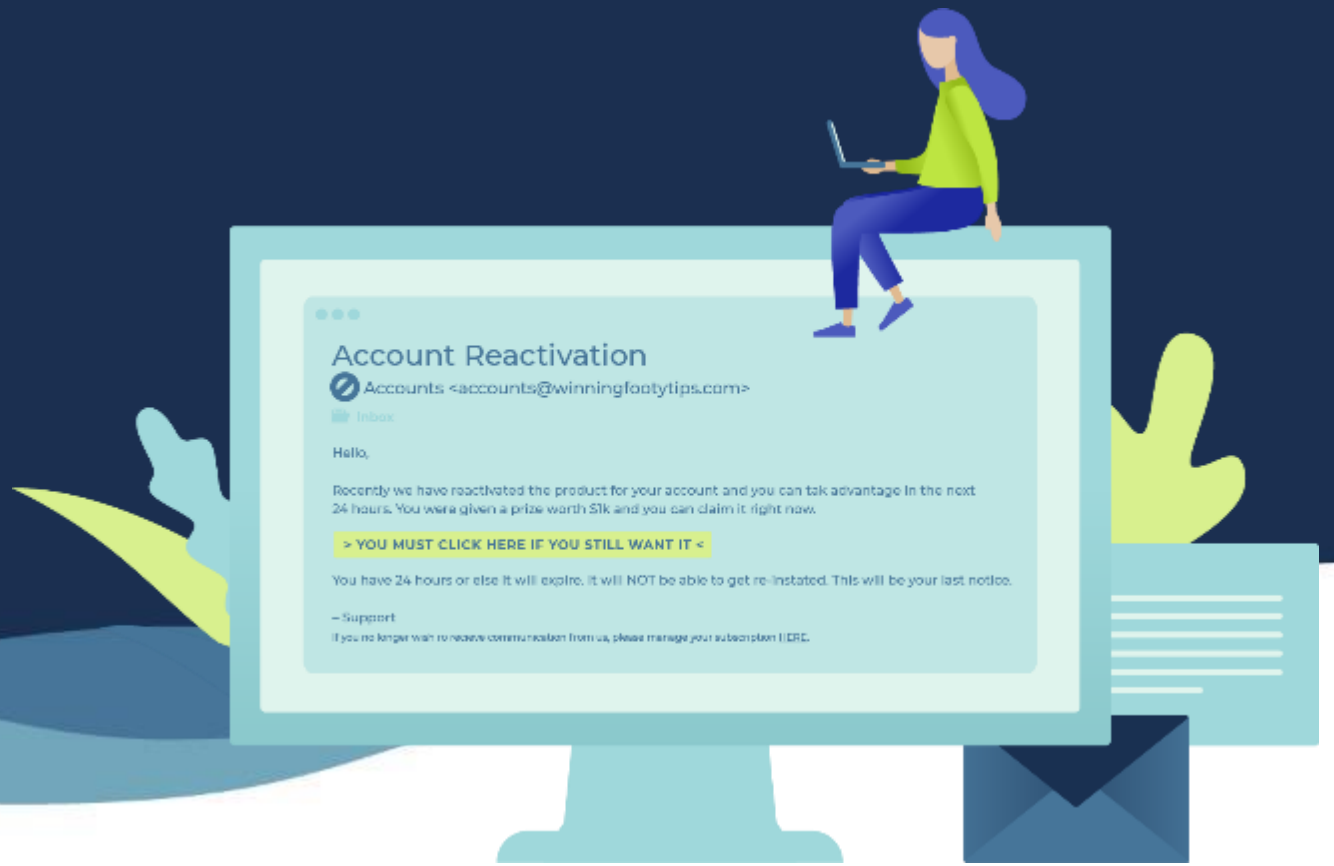
N = New Course

*Course length up to 10 min

PUBLIC

# S.C.A.M. Series

1. S.C.A.M. 101 (gain knowledge - 20 min)
2. S.C.A.M. 201 (apply knowledge - 15 min)
3. S.C.A.M. 301 (create awareness & increase ability - 10min)
4. S.C.A.M. Family Edition (7 min)



# S.C.A.M. 101

Gain phishing knowledge! The first of the S.C.A.M. series of courses, S.C.A.M. 101 introduces learners to basic S.C.A.M. (Sender, Content, Action, Manage) phishing concepts. Employees will understand basic terminology and explore the different approaches scammers use to trick people.

**Level** Beginner
**Duration** 20 Minutes
**Pre-Requisites** N/A
**Target Audience** All Staff

## Learning Outcomes

1. Explain how to scan the **S**ender of an email
2. Explain how to scan the **C**ontents of an email
3. Explain how to scan for **A**ction in the email
4. Discuss how to **M**anage phishing emails


PUBLIC

LITE

# S.C.A.M. 201

S.C.A.M. 201 aims to increase employee's phishing knowledge and enhance their skill in actively analysing and identify phishing emails.

**Level** Intermediate
**Duration** 15 Minutes
**Pre-Requisites** S.C.A.M. 101
**Target Audience** All Staff

## Learning Outcomes

1. Recall basic S.C.A.M. knowledge
2. Understand the structure of a web address
3. Differentiate between real and fake domain names
4. Understand Spear Phishing
5. List the different click-bait tactics used by scammers
6. Identify a Sense of Urgency, Curiosity, and Authority
7. Explain how to report a S.C.A.M. email


PUBLIC

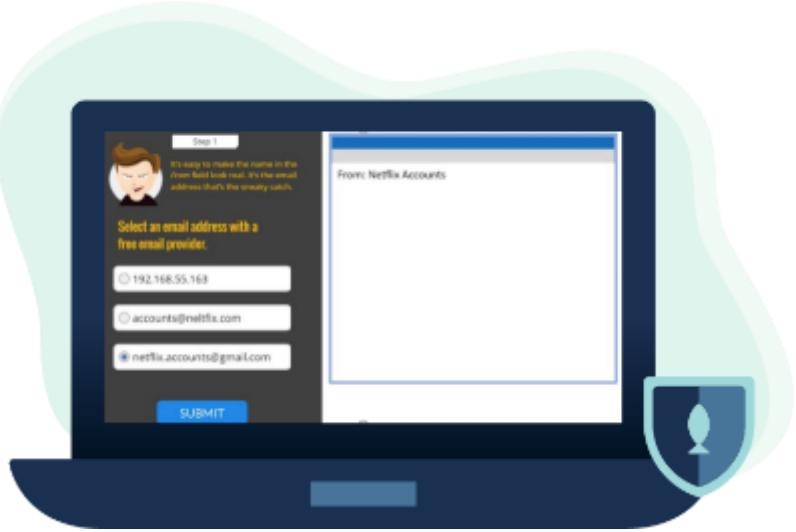
# S.C.A.M. 301

This course offers scenario-based learning and role-playing activities, where employees will take on the role of teacher and scammer. This approach helps staff solidify their phishing knowledge whilst gaining a deeper understanding of how phishing emails are constructed and used.

**Level** Intermediate
**Duration** 10 Minutes
**Pre-Requisites** S.C.A.M. 201
**Target Audience** All Staff

## Learning Outcomes

1. Explain the basics of phishing to a colleague
2. Design a phishing email
3. Help a colleague identify a scam email
4. Explain why an email is scam




PUBLIC

LITE

# S.C.A.M. 101 - Family Edition

Phishing doesn't only happen in the workplace. Ensure your staff and their families are protected at home!  S.C.A.M. 101 Family Edition introduces learners to basic S.C.A.M. (Sender, Content, Action, Manage) phishing concepts, terminology and the different approaches scammers use to trick people.

**Level** Beginner
**Duration** 7 Minutes
**Pre-Requisites** N/A
**Target Audience** Staff's Family

## Learning Outcomes

1. Explain how to scan the **S**ender of an email
2. Explain how to scan the **C**ontents of an email
3. Explain how to scan for **A**ction in the email
4. Discuss how to **M**anage phishing emails


PUBLIC

LITE

# S.C.A.M. Series Feedback

**87%**
employee satisfaction

**83%**
learnt something new

> "Very Informative, really highlights just how tricky [scammers] can be and what lengths they go to trick you."

> "Well done making a very dry subject as fun as possible!"

> "The style and tone was very engaging. It managed to pack in a lot of information in very easy to digest chunks.
>
> I liked the mix of characters, instruction and quizzes. I really enjoyed the training and I learned a lot. Thank you!"

*Feedback based on learner surveys for S.C.A.M. 101, 201 and 301 August 2020 to February 2021

# Keep Secure Series

**Keep Secure Series (10min each)**

1. Security Foundations
2. Cyber-Attack Evolutions
3. Social Engineering
4. Online & Remote Threats
5. Internal Threats
6. KSec5 Framework / Making Intelligent, Ongoing Security Decisions

**Keep Secure Mini-Series (7 min each)**

1. Security Foundations
2. Social Engineering
3. 5 Rules to Keep Secure

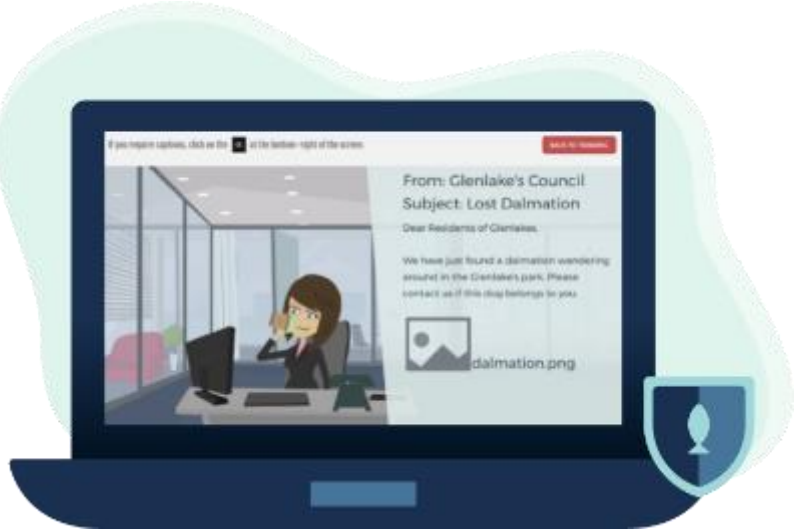
# Keep Secure Series

Our Keep Secure Series aims to create general security awareness among staff by providing the knowledge, context and framework to make smarter, more calculated security decisions.

**Level** Beginner
**Duration** 10 Minutes per Module
**Total Modules** 6
**Target Audience** All Staff

## Keep Secure Series Modules

1. Security Foundations
2. Cyber-Attack Evolutions
3. Social Engineering
4. Online & Remote Threats
5. Internal Threats
6. Keep Secure Framework (KSec) - Making Intelligent, Ongoing Security Decisions




PUBLIC

# Keep Secure Mini-Series

Our Keep Secure Mini-Series is recommended as a 3-part general security awareness refresher series following the full Keep Secure Series.

**Level** Beginner
**Duration** 7 Minutes per Module
**Total Modules** 3
**Target Audience** All Staff

## Keep Secure Mini-Series

1. Security Foundations
2. Social Engineering
3. 5 Rules to Keep Secure (KSec)

# General Security Awareness

1. An Introduction to Information Security
2. Bring Your Own Device (BYOD)
3. Business Email Compromise
4. Cloud Security
5. Email Security
6. Handling Sensitive Information
7. Information Classification
8. Information Security at Work
9. Laptop Security
10. Mobile Phones and Tablets
11. Passwords and Passphrases
12. Personal Information
13. Protecting Credit Card Information
14. Protecting your Digital Identity
15. Safety Online
16. Scams and Social Engineering
17. Security Incidents
18. Security in the Workplace
19. Situational Awareness
20. Smishing
21. Social Media
22. Vishing
23. WiFi

New Course

# An Introduction To Information Security

Secure your information at home, at work and when you are on the go. Ensure your staff understand the rules that define information security and the role that they play in protecting the organisation's information.

**Level** Beginner
**Duration** 5 Minutes
**Target Audience** All Staff

## Learning Outcomes

1. Explain the importance of information security
2. Apply the rules of Confidentiality, Integrity and Availability to secure information
3. Explore ways to secure information at work and at home


PUBLIC

PREMIUM

New Course

# Bring Your Own Device

Bring your own device (BYOD) provides familiarity and ease for users but having diverse technologies can cause significant disruptions to organisation security. Ensure your staff understand the security measures to take when using their own device.

**Level** Beginner
**Duration** 5 Minutes
**Target Audience** All Staff

## Learning Outcomes

1. Explain what BYOD means
2. List some of the benefits to BYOD
3. Discuss the vulnerabilities of BYOD

PUBLIC

PREMIUM

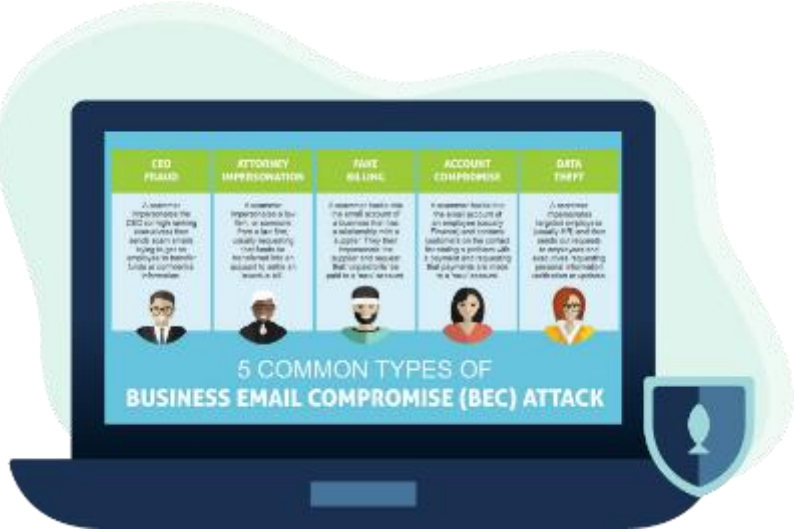
# Business Email Compromise

Business Email Compromise (BEC) aims to target staff who have access to sensitive company information or company finances. Employees will discover the simple, and highly effective scams using malware or social engineering (or both) in this short course.

**Level** Beginner
**Duration** 7 Minutes
**Target Audience** All Staff

## Learning Outcomes

1. CEO Fraud
2. Data Theft
3. Attorney Compliance
4. Fake Billing
5. Account Compromise




PUBLIC

PREMIUM

New Course

# Cloud Security

The cloud is a convenient and cost-effective way to store information but it does come with security risks. This course lists some of the risks associated with cloud computing and offers some tips on securing your information when using the cloud.

**Level** Beginner
**Duration** 5 Minutes
**Target Audience** All Staff

## Learning Outcomes

1. Explain what cloud security (and storage) entails
2. Discuss some of the common risks and benefits to cloud security
3. List some of the best practices that can be applied when considering (or using) cloud security

PUBLIC

PREMIUM

New Course

# Email Security

Email is a great tool for communicating, both personally and professionally, but there can be issues when you blend the two worlds together. Give your staff clarity on how they can protect the organisation and themselves from the always evolving danger of cyber threats.

**Level** Beginner
**Duration** 5 Minutes
**Target Audience** All Staff

## Learning Outcomes

1. Discuss the pitfalls of mixing work & personal email
2. Explain some examples of email compromise
3. Explain ways to keep information safe when using email


PUBLIC

PREMIUM

New Course

# Handling Sensitive Information

Sensitive information is a valuable commodity. It ranges from low to high classifications, with official markings designed to help organisations manage and secure their sensitive information. This short course offers some tips on how to handle and protect sensitive information.

**Level** Beginner
**Duration** 5 Minutes
**Target Audience** All Staff

## Learning Outcomes

1. Discuss the importance of handling sensitive information
2. Identify the different categories of sensitive information

PUBLIC

PREMIUM

New Course

# Information Classification

Information classification ensures everyone in an organisation easily understands who can and should have access to different types of information. Introduce your staff to this classification and labelling concept.

**Level** Beginner
**Duration** 5 Minutes
**Target Audience** All Staff

## Learning Outcomes

1. Discuss the importance of classifying information
2. Identify the different classification markings

PUBLIC

PREMIUM

New Course

# Information Security At Home

With remote working more prevalent your organisation's valuable information is now mobile.  Ensure your staff understand how to implement information security practices at home.

**Level** Beginner
**Duration** 5 Minutes
**Target Audience** All Staff

## Learning Outcomes

1. Discuss the importance of securing your information at home
2. Explain ways to implement security measures at home

PUBLIC

PREMIUM

New Course

# Laptop Security

Make sure your staff understand the security responsibilities of their work laptops. From information security, proper storage and appropriate use, your staff will leave this course with a solid understanding of how to protect this important piece of company hardware.

**Level** Beginner
**Duration** 5 Minutes
**Target Audience** All Staff

## Learning Outcomes

1. Discuss the importance of protecting your laptop
2. List the ways to protect your laptop


PUBLIC

PREMIUM

New Course

# Mobile Phones And Tablets

As our dependence on mobile phones and devices increases, so too should our security. Old and new security threats pop up each day specifically targeting mobile devices. Ensure your staff understand how to best protect their mobile devices at work and home.

**Level** Beginner
**Duration** 5 Minutes
**Target Audience** All Staff

## Learning Outcomes

1. Discuss the common security threats for mobile devices
2. List ways to prevent mobile device attacks and/or theft


PUBLIC

PREMIUM

New Course

# Passwords and Passphrases

Passwords are the primary means to authenticating and accessing systems within organisations and at home.  Ensure your staff understand the important role of passwords in keeping information safe and secure.

**Level** Beginner
**Duration** 5 Minutes
**Target Audience** All Staff

## Learning Outcomes

1. Differentiate between passwords and passphrases
2. List secure ways to manage and update passwords and passphrases

PUBLIC

PREMIUM

New Course

# Personal Information

Sensitive staff information is a valuable commodity for organisations. This course will help your staff understand how to keep their own and other people's sensitive information protected.

**Level** Beginner
**Duration** 5 Minutes
**Target Audience** All Staff

## Learning Outcomes

1. Explain what personal information means
2. Discuss why it's important to protect the customer's personal information
3. List the common things that can occur if a hacker was able to access and utilise the customers personal information


PUBLIC

PREMIUM

New Course

# Protecting Credit Card Information

If your staff accept or manage credit cards details at work, ensure they know how to protect those details.  Employees will cover the common threats scammers use to steal credit card information and learn key safety measures for corporate and personal credit cards.

**Level** Beginner
**Duration** 5 Minutes
**Target Audience** All Staff

## Learning Outcomes

1. Explain how to protect credit card details
2. Discuss some of the ways credit card information could be intercepted by scammers
3. List some of the safety measures to ensure credit card data is kept secure


PUBLIC

PREMIUM

New Course

# Protecting Your Digital Identity

Your digital identity helps prove who you are online. Safeguard your organisation and staff by educating them about safe cyber practices when accessing the internet.

**Level** Beginner
**Duration** 5 Minutes
**Target Audience** All Staff

## Learning Outcomes

1. Explain the value of a person's digital identity
2. Discuss the ways that digital identity can be compromised
3. List ways to protect your digital identity

PUBLIC

PREMIUM

New Course

# Safety Online

Using any device to access the internet can lead to security breaches. This course provides employees tips on how to stay safe online and avoid any security breaches.

**Level** Beginner
**Duration** 5 Minutes
**Target Audience** All Staff

## Learning Outcomes

1. Explain the importance of following organisational protocols when accessing the internet
2. List online safety measures which can be implemented across an organisation


PUBLIC

PREMIUM

New Course

# Scams and Social Engineering

Social engineering is the dark art of manipulating people into performing actions or divulging information. This course identifies some common signs of scams via social engineering. Staff will learn how to protect themselves and the organisation from social engineering.

**Level** Beginner
**Duration** 5 Minutes
**Target Audience** All Staff

## Learning Outcomes

1. Explain what social engineering is
2. Discuss some of the techniques that social engineers utilise
3. List some of the ways to keep information safe when dealing with sensitive information

PUBLIC

PREMIUM

New Course

# Security Incidents

Security is everyone's responsibility. This course aims to highlight the dangers of security incidents and provide your staff with tips on how to protect themselves and the organisation.

**Level** Beginner
**Duration** 5 Minutes
**Target Audience** All Staff

## Learning Outcomes

1. Explain why it is important to communicate a security incident
2. Discuss some of the things that would trigger the need to report a security incident
3. List some of the things that could go wrong if a security incident was not reported


PUBLIC

PREMIUM

New Course

# Security In The Workplace

Most security breaches usually happen by human error. Empower your staff with best practices on how to keep information secure in the workplace.

**Level** Beginner
**Duration** 5 Minutes
**Target Audience** All Staff

## Learning Outcomes

1. Explain the importance of maintaining a secure workplace
2. Discuss ways sensitive information can be compromised in an unsecure workplace
3. List ways to keep the workplace secure


PUBLIC

PREMIUM

New Course

# Situational Awareness

We need to be careful of where, when and to whom we divulge information. This short course looks at the importance of implementing situational awareness effectively.

**Level** Beginner
**Duration** 5 Minutes
**Target Audience** All Staff

## Learning Outcomes

1. Explain what situational awareness is and why it is important
2. List ways that assist staff in becoming more situationally aware

PUBLIC

PREMIUM

# Smishing

An emerging threat in cyber security is SMS Phishing, also known as Smishing. Scammers developed Smishing tactics to tap into the trusting nature of text messaging. Empower your staff to spot a Smishing attack.

**Level** Beginner
**Duration** 7 Minutes
**Target Audience** All Staff

## Learning Outcomes

1. Explain Smishing
2. Discuss common tactics used in Smishing attacks
3. Explain how to manage suspicious text messages
4. Explain how to prevent Smishing attacks

PUBLIC

PREMIUM

New Course

# Social Media

Social media has become a regular part of our lives. Your staff should be aware of the risks of sharing information on social media and how to apply safety measures to protect themselves, the organisation and their families.

**Level** Beginner
**Duration** 5 Minutes
**Target Audience** All Staff

## Learning Outcomes

1. Discuss the benefits and pitfalls of sharing information on social media
2. List some of the safety measures you can implement to keep your information safe from prying eyes

PUBLIC

PREMIUM

New Course

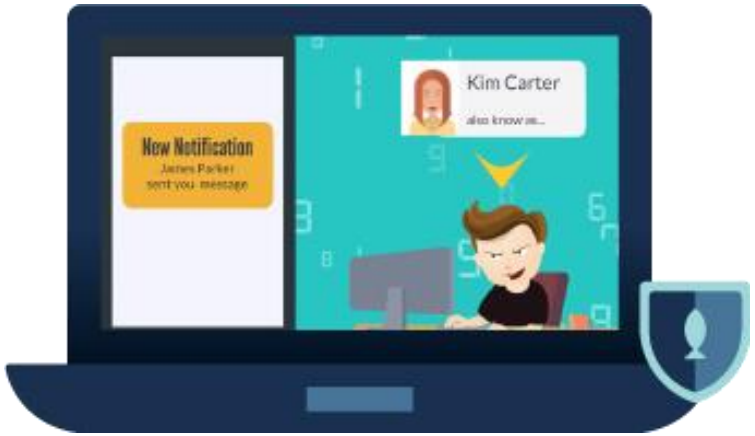
# Vishing

Cyber criminals use voice calls to convince their victims to give up personal and/or confidential. Your staff need to be aware of the savvy social engineering tactics and trends to how to protect themselves, their families and the organisation from becoming a victim of this type of scam.

**Level** Beginner
**Duration** 7 Minutes
**Target Audience** All Staff

## Learning Outcomes

1. Explain what Vishing is
2. Explain why it's important to be aware of Vishing scams
3. Discuss how to protect yourself from Vishing scams




PUBLIC

PREMIUM

New Course

# Wi-Fi

Wi-Fi can be very convenient but also very dangerous. Educate your staff about the risks of Wi-Fi and how to utilise this option safely.

**Level** Beginner
**Duration** 5 Minutes
**Target Audience** All Staff

## Learning Outcomes

1. Explain the best practice approach to take when using free public Wi-Fi hotspots
2. Discuss the overall risks posed when choosing to connect to free public Wi-Fi hotspots


PUBLIC

PREMIUM

# Government Guidelines

1. Removable Media
2. Privileged Access Management
3. Secure by Design
4. *Security Incident Response

New Course

# Removeable Media

Removable Media refers to any type of portable storage device that allows you to transfer, store or back-up data without powering off your computer. Ensure your staff understand and are aware of their responsibility of having access to removable media devices, ultimately protecting the organisation and themselves.

**Level** Beginner
**Duration** 10 Minutes
**Target Audience** All Staff

## Learning Outcomes

1. Explain the classifications of removeable media
2. Discuss the ramifications of misuse
3. Discuss the conditions to use removeable media
4. Explain how to report a removeable media incident


PUBLIC

PREMIUM

New Course

# Privileged Access Management (PAM)

Users with administrative privileges for operating systems and applications can make significant changes to their configuration and operation, bypass critical security settings and access sensitive information. Ensure staff with PAM understand their security obligations.

**Level** Beginner
**Duration** 10 Minutes
**Target Audience** All Staff

## Learning Outcomes

1. Explain Privileged Access Management (PAM)
2. List the obligations for a privileged user
3. Explain how to request privileged system access

PUBLIC

PREMIUM

New Course

# Secure by Design

As systems advance, it becomes increasingly difficult to add effective security layers. Secure by Design embeds security from the start to minimise risk and vulnerabilities. Staff will gain an understanding of the Secure by Design process and be empowered to incorporate cyber resilience into new and existing systems.

**Level** Beginner
**Duration** 10 Minutes
**Target Audience** System Owners, Project Managers, Programme Managers

## Learning Outcomes

1. Explain Secure by Design meaning and importance
2. Discuss Secure by Design implementation
3. Apply a risk-based approach to projects
4. Explain incorporating security into design


PUBLIC

PREMIUM

New Course

# Security Incident Response

Help all staff identify a security incident and show them what to do should they encounter one. By understanding how to respond to security incidents, staff will be protecting the organisation, computer network, systems, people, information, assets and themselves from any malicious attempts.

**Level** Beginner
**Duration** 10 Minutes
**Target Audience** System Owners, Project Managers, Programme Managers

## Learning Outcomes

1. Explain what a security incident is
2. Discuss the classifications of security incidents
3. *Explain how to report a security incident


***Note**: This course includes a free email comms/poster that you can customise with your company's specific instructions outlining how to report a security incident. Instead of staff having to search for this important information from a course, we recommend that after the training has been scheduled, send this out to staff to make it easy to quickly reference this information from your email comms, as and when they need to.

PUBLIC

PREMIUM

New Course

# Information Privacy and Security

When dealing with personal information, it is imperative that safety measures are taken to protect the information and to be aware of the risks associated with security breaches and incidents. This course explores the Australian Privacy Principals that provide guidelines on handling personal information throughout the information lifecycle and provides tips on how to prevent loss of information.

**Level** Beginner
**Duration** 10 Minutes
**Target Audience** All Staff

## Learning Outcomes

1. Differentiate between personal and sensitive information
2. List ways to handle information with care
3. Explain how to handle a security incident


PUBLIC

PREMIUM


PhriendlyPhishing.com

To add additional courses to your subscription contact:
support@phriendlyphishing.com | 1300 407 682