



Security Awareness Training

encription limited

Security Awareness Seminars



encription limited
The Stables
White Lodge
Bever
Worcester
WR3 7RQ

01905 754440
www.encription.co.uk

July 2007

1





Security Awareness Training

Staff are the major weaknesses in IT and information security.

They can unwittingly give away confidential information, as well as putting the data at risk by not taking appropriate precautions.

How can a person be disciplined for unacceptable use of IT if they have not been formally made aware of what is acceptable and what is not?

This seminar addresses all of these issues in just a morning or an afternoon, it can also be used as part of an induction programme and in conjunction with encription's on-line security awareness training.

Designed for:

Anyone who uses IT or deals with confidential information.

Duration

Each session will last 2.5 hours

At the end of each seminar attendees will:

- ✓ Have an understanding of the types of security attack that can occur and will know what to look out for.
- ✓ Know what to do with sensitive information
- ✓ Know how to protect information when using removable media (USB Stick), emails, phone and fax communications
- ✓ Understand the risks of WiFi and PDA's (e.g. Blackberry)
- ✓ Be aware of the company's acceptable use and email policy.

Certification



Attendees will be awarded a certificate showing that they have undertaken this training and are rated as encription verified in IT security awareness.

July 2007

2





Security Awareness Training

MODULES

Information Security Basics

Security principles
Potential impact
Data sensitivity
Security Controls

Access Control

Introduction
Privileges
Types of Access control
Authentication and accountability
Usernames and passwords
Password policy
Overcoming problems with passwords

Appropriate and Personal Use

Introduction
Examples of inappropriate use (Based on client's own policy)
Equipment
Consequences of non-compliance

Mobile Computing

Introduction
Risks
Procedures for use
Best practices
Wireless Networks
Data security
Do's and Don'ts

Intrusions and Malicious Software

Introduction
Defence – removable media etc
Malicious software
Viruses
Best practices
Social engineering – further defence

Email Security

Introduction
Steps to improve email security
Privacy
Email Spoofing
Phishing
Hoaxes and Spam



Security Awareness Training

Internet Security

Introduction
Software downloads
Internet use policy (Based on client's own policy)
Identity theft
Messaging and chat

Information Management and Data

Introduction
Back ups
Sensitive information
Procedures
Disposing of sensitive information
Privacy
Hazards
Securing your workstation
Securing printed output
Fax and phone
Waste disposal

Incident Handling and Reporting

Introduction
Examples of incidents
Symptoms of an incident
Incident reporting

Remote Access

Introduction
Do's and Don'ts

Physical Security

Introduction
Physical, technical, environmental and administrative controls

Relevant handouts will be provided