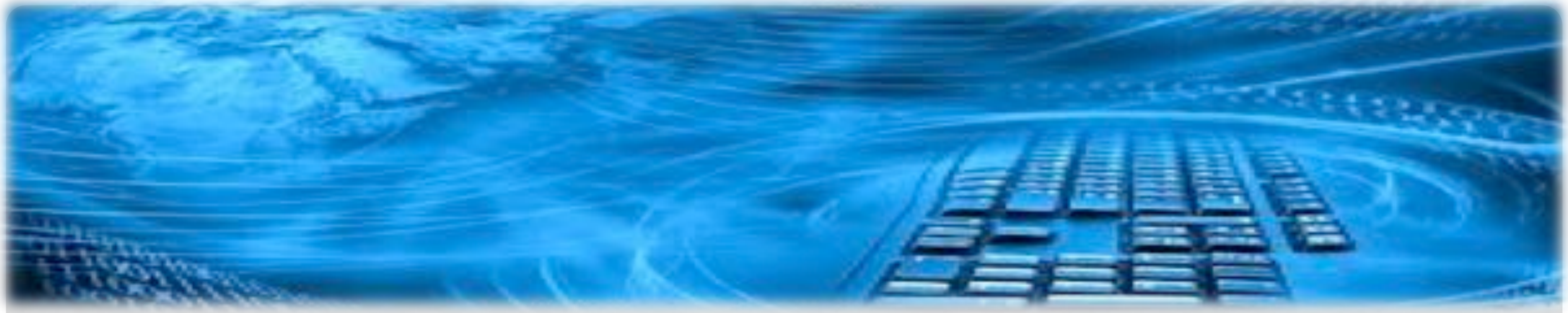


cyberm

Security Awareness Program

THE REQUIREMENT

"Technology alone cannot address one of the most difficult problems to manage in security: the human factor."

AREAS OF GROWING CONCERN

cyberm

Mobile

Social Engineering

Social Media

MOBILE

Business is now mobile—and mobile is more vulnerable

- Executives and employees use personal smartphones and tablets for business.*
- Two thirds of users don't use a security solution for their mobile device.
- Website blocks based on corporate policies get triggered more often by workers who are on the road versus those in their offices.
- Staff have lost their mobile device or had it stolen.

SOCIAL ENGINEERING

The human element is the weakest link

- The art of manipulating people into performing actions or divulging confidential information for fraud, computer access, or gathering information.
- People are the weakness attackers try to exploit
- Malicious attacks are based on social engineering
- Technology can’t defend against social engineering

SOCIAL MEDIA

Workplace communications now include social media

- Facebook: Almost 2 billion monthly active users
- YouTube: Billions of hours of videos viewed each month
- Business-related sites like LinkedIn increase workplace vulnerability.
- Users are only as secure as their circle of social network friends (and friends of friends).
- Users accept friend requests from people they don’t know.
- Social network users fall victim to cybercrime on social networking platforms.
- Social Networking Attacks by:
  - blogs & web communications
  - hosted or personal hosted site

SECURITY AWARENESS WORKSHOPS

GENERAL USERS WORKSHOP

- **Duration:** 2-4 Hours
- **Audience:** All staff
- **Topics:**
  - Defend Yourself Against Malware
  - Good Password Practice
  - Secure Use of E-Mail
  - Safe Surfing
  - Physical Security
  - Social Engineering/Phishing
  - Social Media Security
  - Mobile Devices Security

MANAGEMENT WORKSHOPS

- Duration: 45– 60 Minutes
- Audience: All management staff
- Topics:
  - The Need For Information Security
  - Cost Of No Investment (CONI)
  - Return of Investment (ROI)
  - Financial/Legal Liability
  - ISO27001
  - Data Classification & Ownership
  - Business Continuity

IT STAFF AWARENESS WORKSHOPS

- **Duration:** 8 Hours
- **Audience:** All IT staff
- **Topics:**
  - Introduction to Security Terminology
  - ISO27001 Essentials
  - Risk Assessment
  - Network Security Fundamentals
  - Host Security Fundamentals
  - Security Attacks and Protection
  - Web Security
  - Cryptography

IT Staff Awareness Workshops

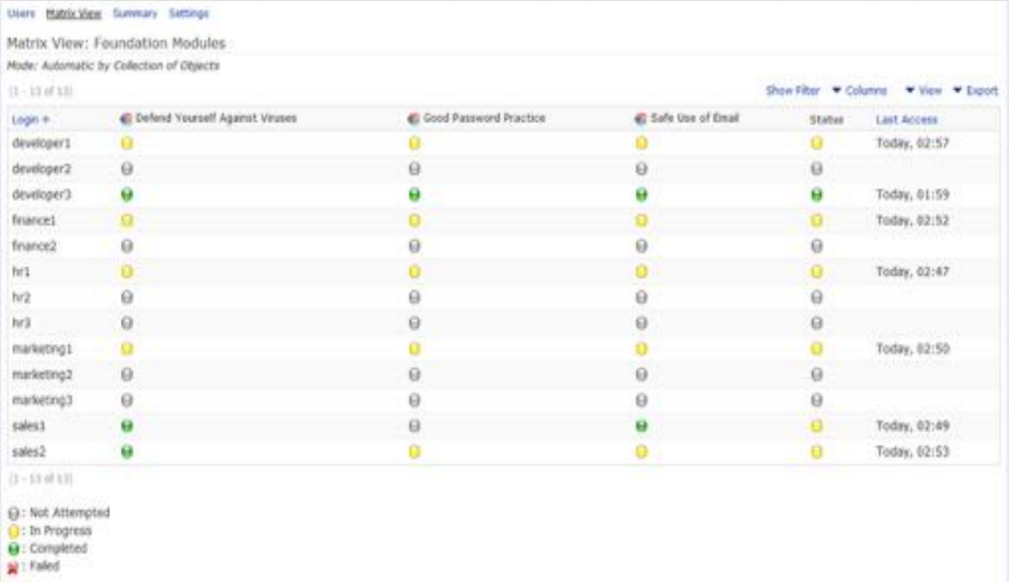
SECURITY AWARENESS TRAINING

OVERVIEW

- Promotes proactive employee behavior to better protect information assets
- Meets regulatory requirements specific to employee security awareness training
- Comprehensive Cloud based training and post-assessment to measure employee understanding (on premise solution available)
- Promotes retention with multiple communication tools:
  - Posters
  - Infographics
  - Email reminders/shots
  - SMS Messages
  - Roll-Ups
  - Videos
  - Games
  - Gifts

FEATURES

- An excellent tool to track the progress of client’s security awareness program.
- Reports outlining who has attended the program
- Evidence of the security awareness program implementation and supports the future ISO27001/2 certification process
- Meets mandated compliance requirements.
- Admin can assign different modules to different Users (or departments)
- Export reports in different formats
- Completion certificates
- Configurable LMS Front page
- Fully SCORM compliant
  - SCORM 1.2
  - SCORM 1.3 (2004)
- Auto E-mail Notifications
- Web 2.0 and Ajax technologies



Matrix View: Foundation Modules

Mode: Automatic by Collection of Objects

[1 - 13 of 13]

Login +	Defend Yourself Against Viruses	Good Password Practice	Safe Use of Email	Status	Last Access
developer1	🟡	🟡	🟡	🟡	Today, 02:57
developer2	○	○	○	○	
developer3	🟢	🟢	🟢	🟢	Today, 01:59
finance1	🟡	🟡	🟡	🟡	Today, 02:52
finance2	○	○	○	○	
hr1	🟡	🟡	🟡	🟡	Today, 02:47
hr2	○	○	○	○	
hr3	○	○	○	○	
marketing1	🟡	🟡	🟡	🟡	Today, 02:50
marketing2	○	○	○	○	
marketing3	○	○	○	○	
sales1	🟢	○	🟢	🟡	Today, 02:49
sales2	🟢	🟡	🟡	🟡	Today, 02:53

[1 - 13 of 13]

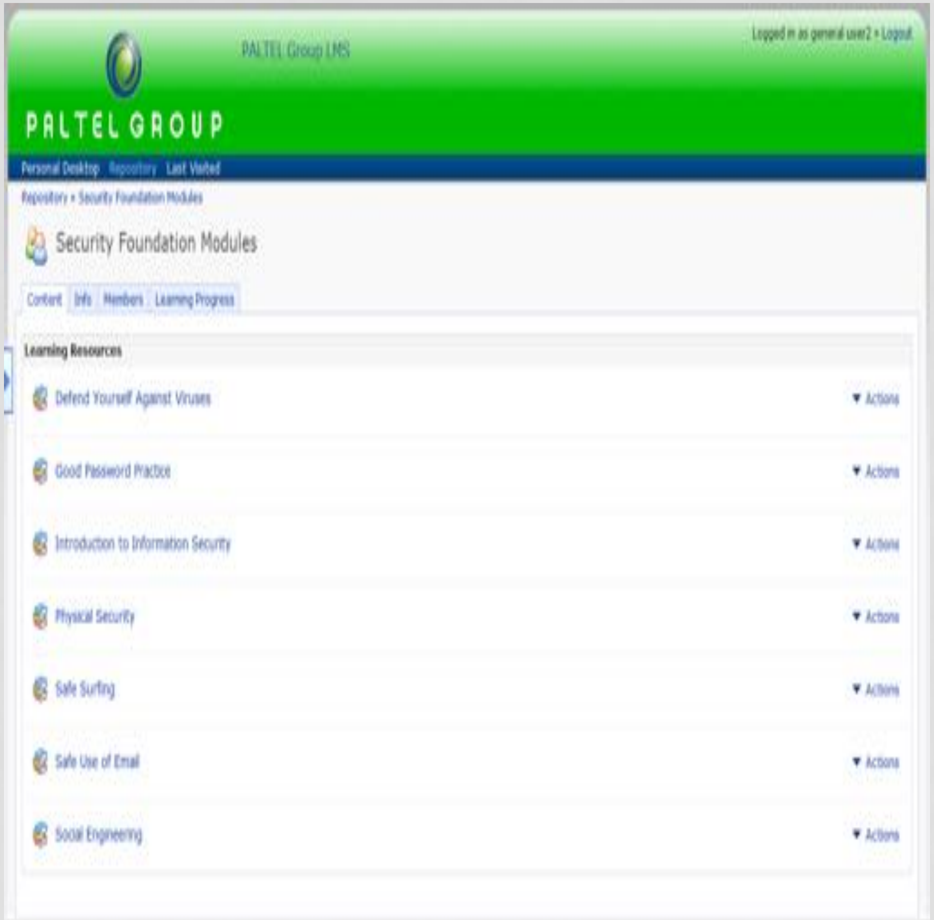
○ : Not Attempted
🟡 : In Progress
🟢 : Completed
✗ : Failed

MODULES

10 Modules Included:

1. Introduction to Information Security
2. Passwords
3. Social Networks
4. Malware
5. Identity Theft
6. Phishing
7. Information Classification
8. Social Engineering
9. Email
10. Clear Desktop Policy

- *Quizzes and Certification*



PALTEL Group LMS

Logged in as general user2 • Logout

PALTEL GROUP

Personal Desktop Repository Last Visited

Repository » Security Foundation Modules

Security Foundation Modules

Content Info Members Learning Progress

Learning Resources

Defend Yourself Against Viruses ▼ Actions

Good Password Practice ▼ Actions

Introduction to Information Security ▼ Actions

Physical Security ▼ Actions

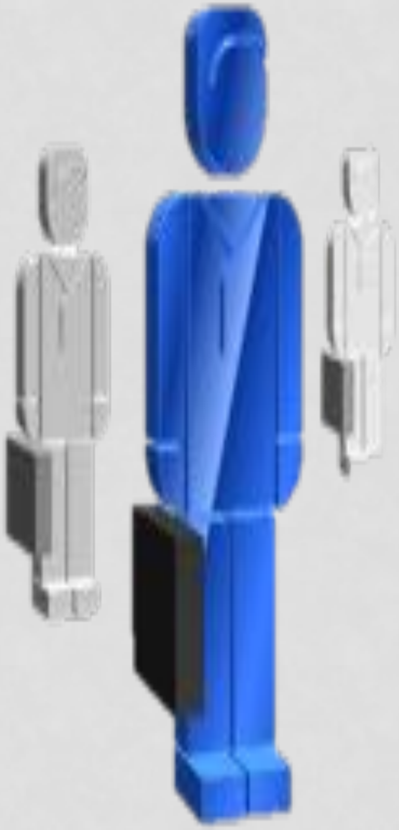
Safe Surfing ▼ Actions

Safe Use of Email ▼ Actions

Social Engineering ▼ Actions

ACCOUNTS MANAGEMENT

- Built-in accounts management
- LDAP full accounts management and integration
- Users self-registration
  - Registration by verification email
  - Registration by administrator approval
  - Manual registration of users by administrator

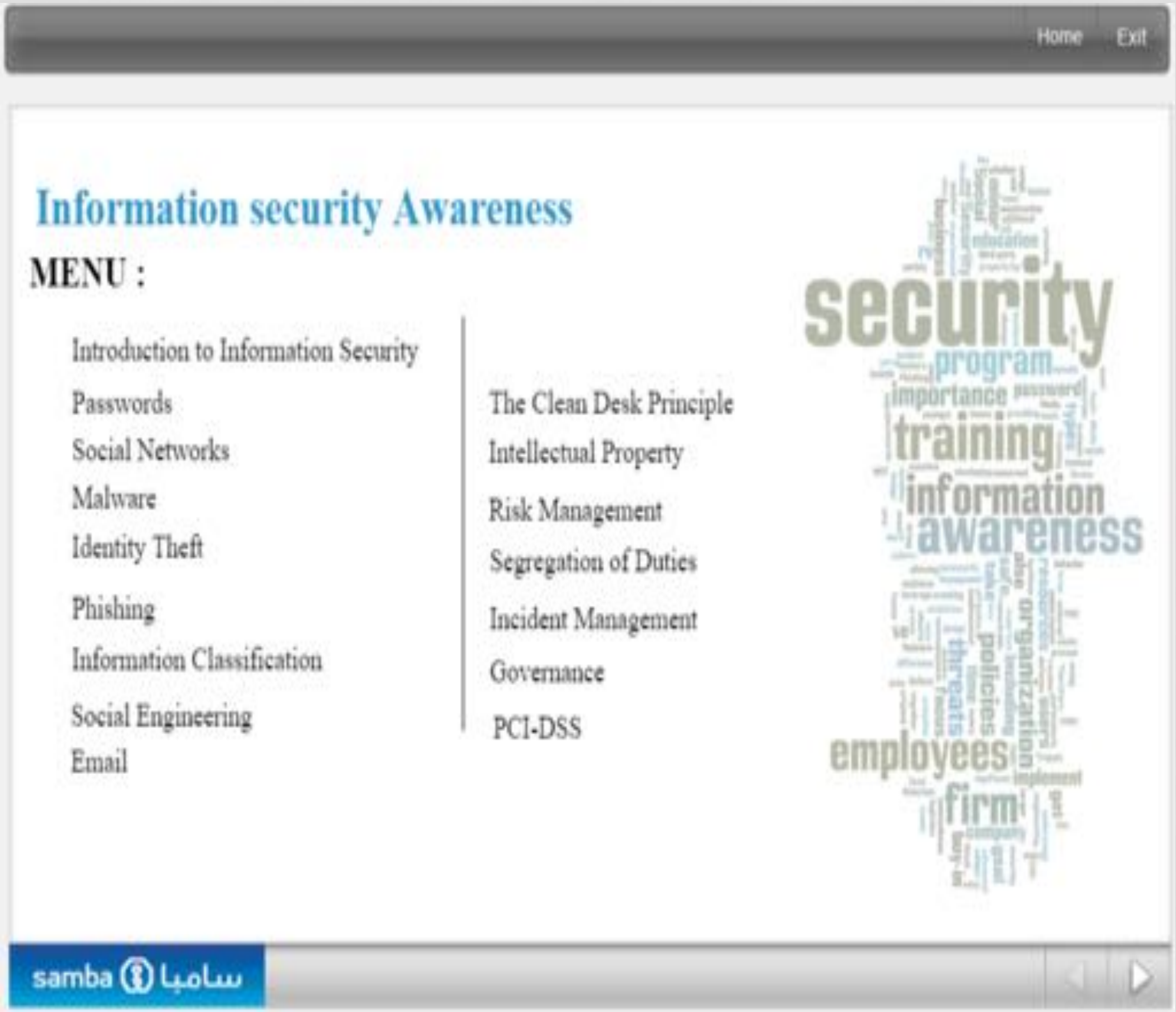


TRACK & REPORT

At any time, management can monitor employees progress

- Track learner performance and grades
- Configure custom grading/assessment scales
- Configure custom items to be graded/assessed
- Export data in different formats
  - CSV
  - XLS
- Track users activity statistics
- Track the learning materials usage statistics
- View reports
  - learner progress report
  - course completion report
  - course materials access report
- Configure criteria and filters for reports
- Export reports in different formats
  - CSV
  - XLS

BRANDING SAMPLE 1

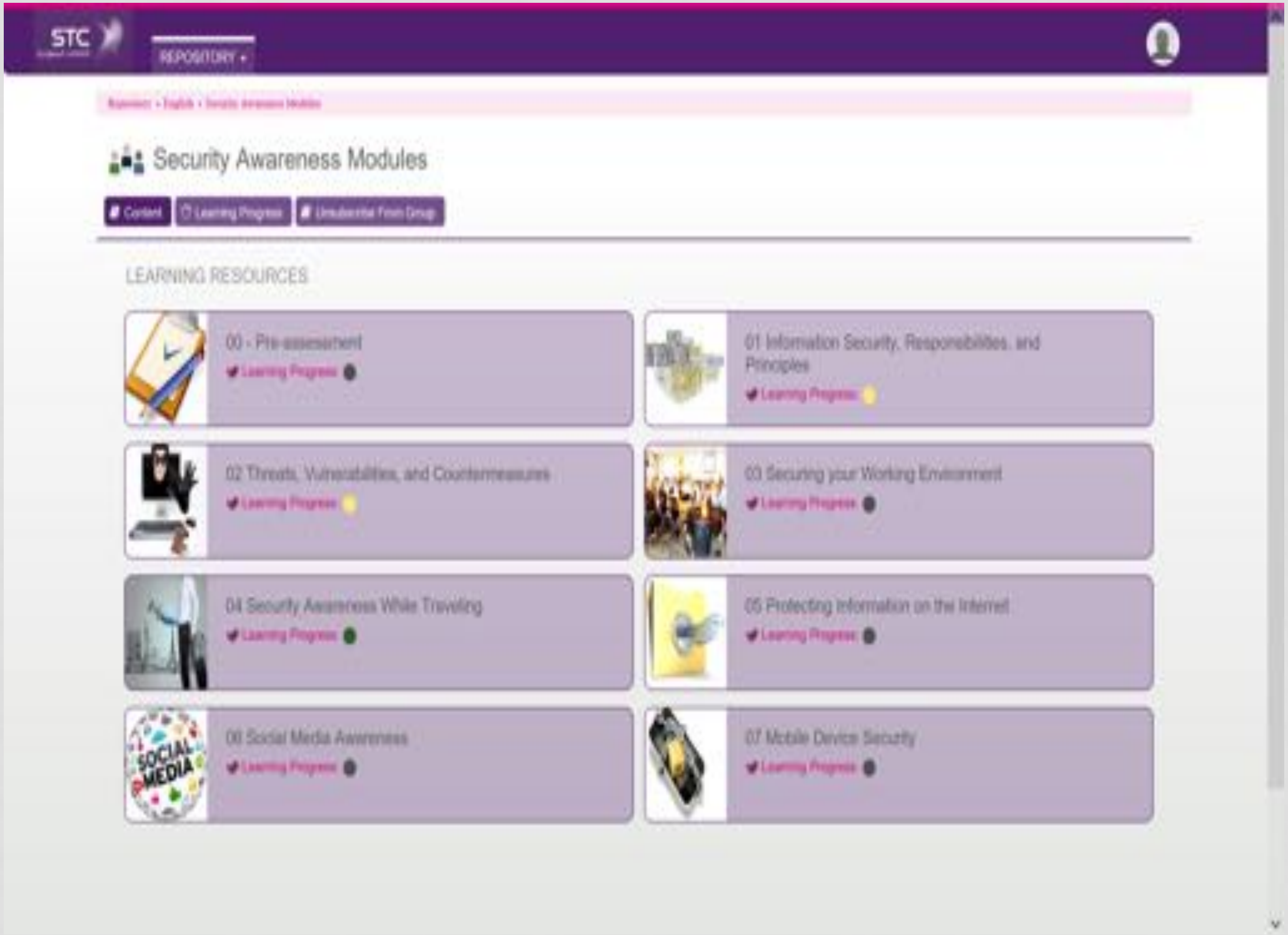


Information security Awareness

MENU :

- Introduction to Information Security
- Passwords
- Social Networks
- Malware
- Identity Theft
- Phishing
- Information Classification
- Social Engineering
- Email
- The Clean Desk Principle
- Intellectual Property
- Risk Management
- Segregation of Duties
- Incident Management
- Governance
- PCI-DSS

BRANDING SAMPLE 2



STC

REPOSITORY ▾

Repository » English » Security Awareness Modules

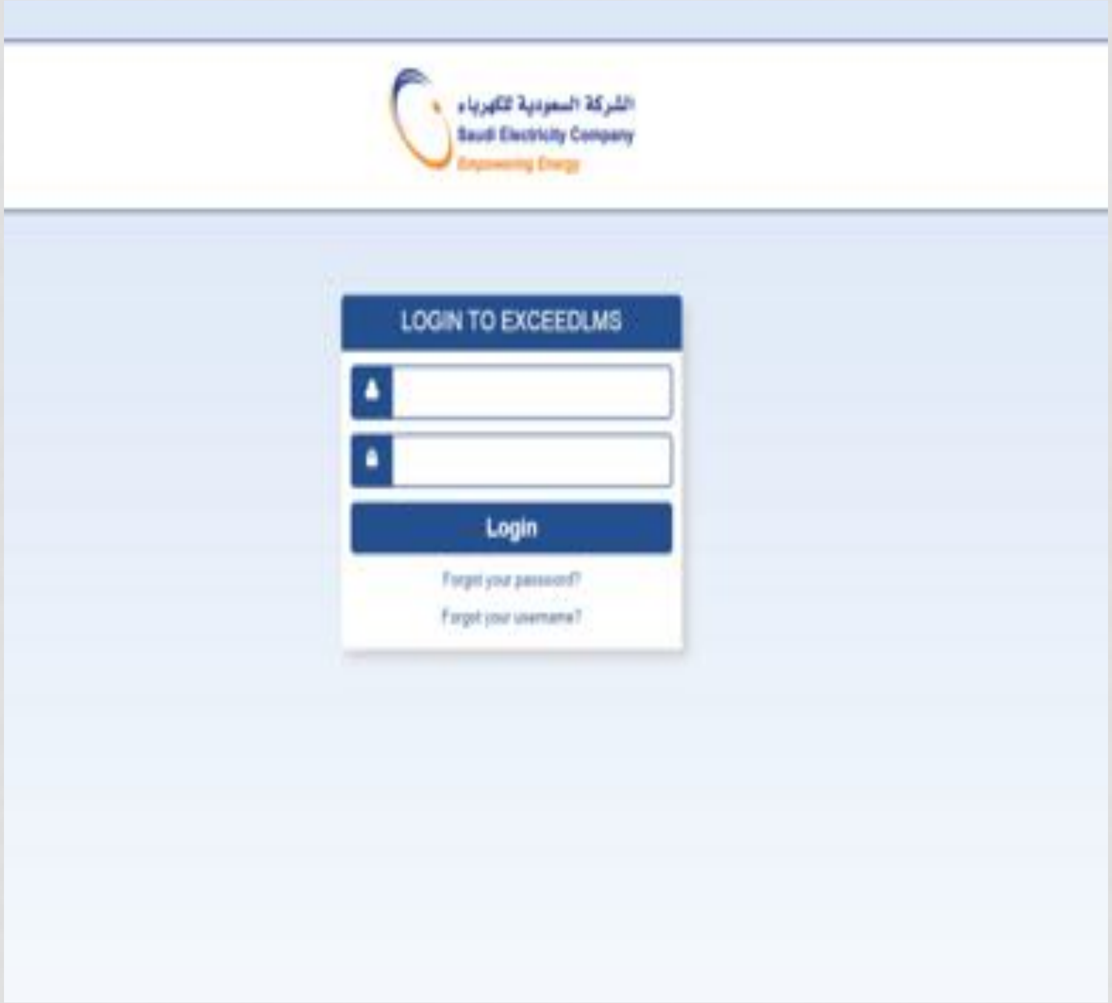
Security Awareness Modules

Content | Learning Progress | Unsubscribe From Group

LEARNING RESOURCES

- 00 - Pre-assessment — Learning Progress ●
- 01 Information Security, Responsibilities, and Principles — Learning Progress ●
- 02 Threats, Vulnerabilities, and Countermeasures — Learning Progress ●
- 03 Securing your Working Environment — Learning Progress ●
- 04 Security Awareness While Traveling — Learning Progress ●
- 05 Protecting Information on the Internet — Learning Progress ●
- 06 Social Media Awareness — Learning Progress ●
- 07 Mobile Device Security — Learning Progress ●

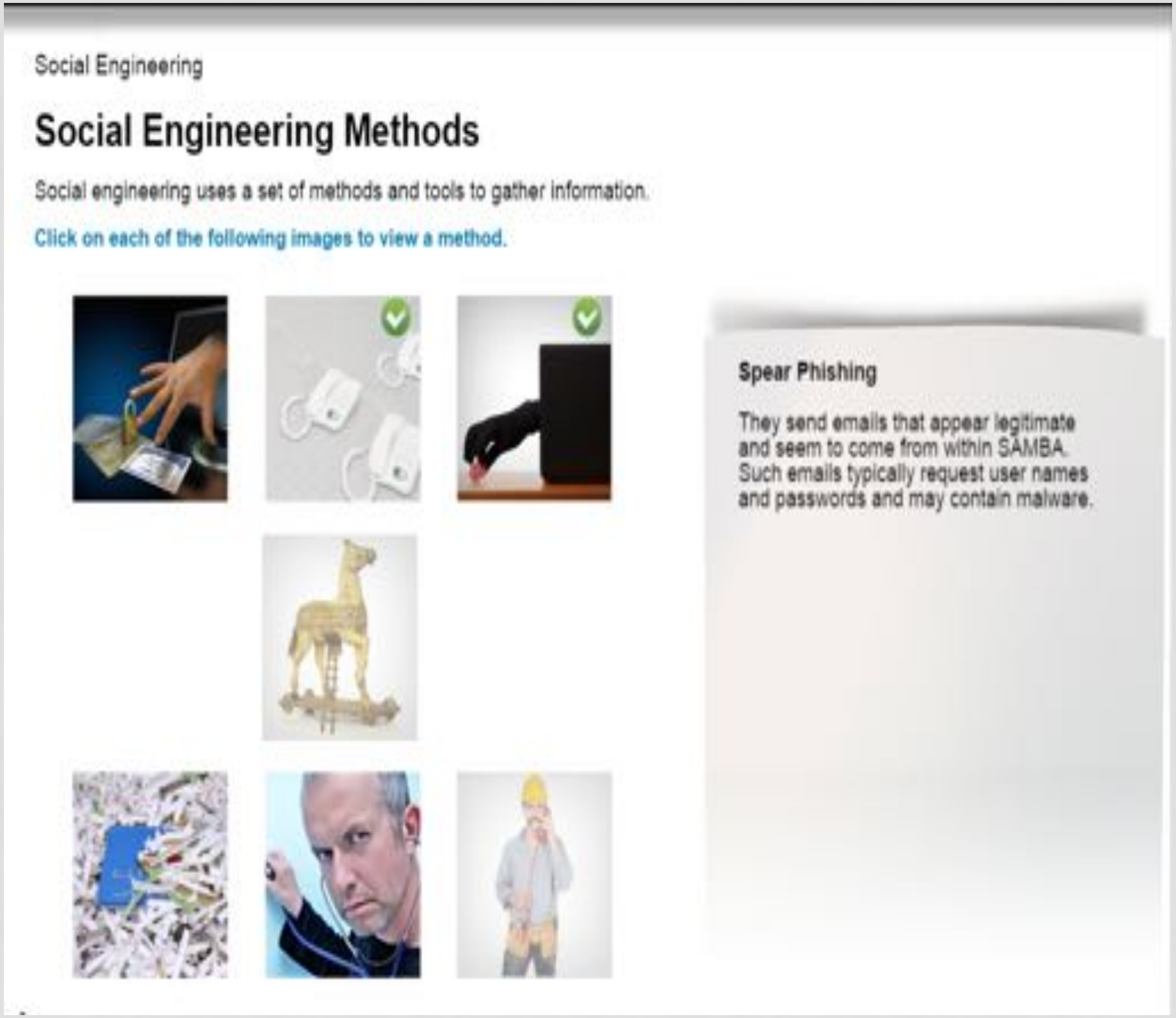
BRANDING SAMPLE 3



الشركة السعودية للكهرباء
Saudi Electricity Company
Empowering Energy

MODULE SAMPLE 1

cyberm



Social Engineering

Social Engineering Methods

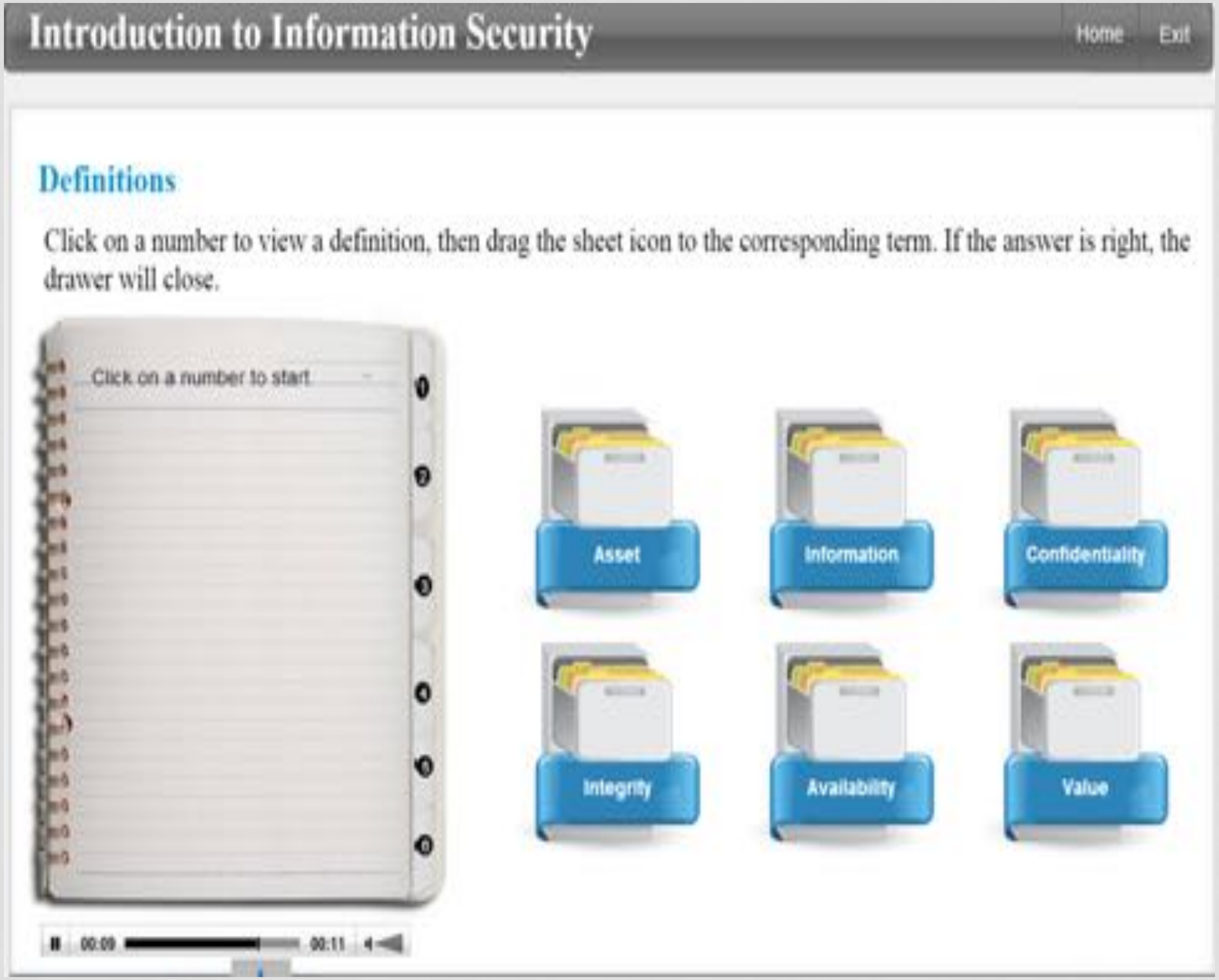
Social engineering uses a set of methods and tools to gather information.

Click on each of the following images to view a method.

Spear Phishing

They send emails that appear legitimate and seem to come from within SAMBA. Such emails typically request user names and passwords and may contain malware.

MODULE SAMPLE 2



Introduction to Information Security

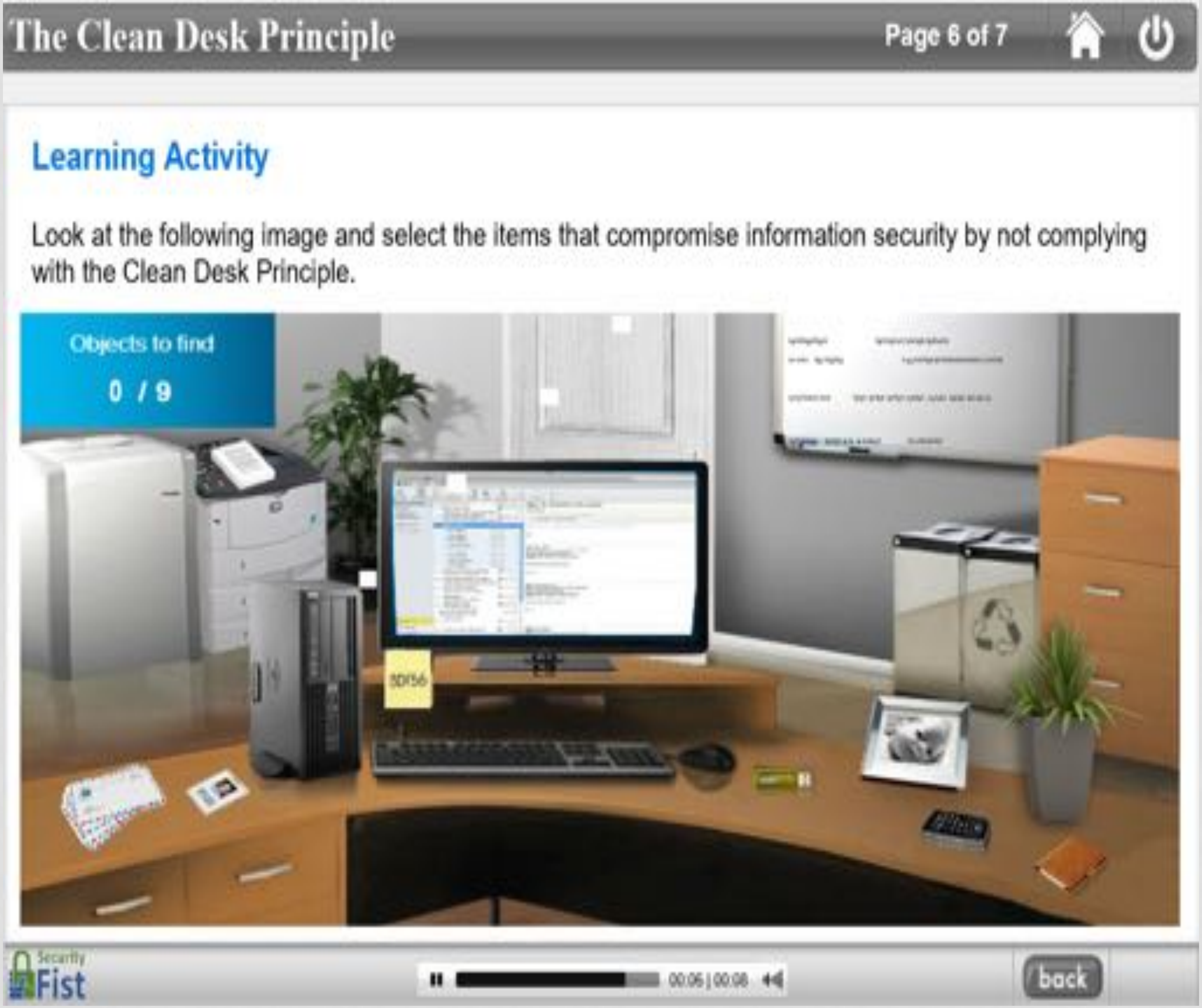
Definitions

Click on a number to view a definition, then drag the sheet icon to the corresponding term. If the answer is right, the drawer will close.

Click on a number to start

VIDEO CLIPS

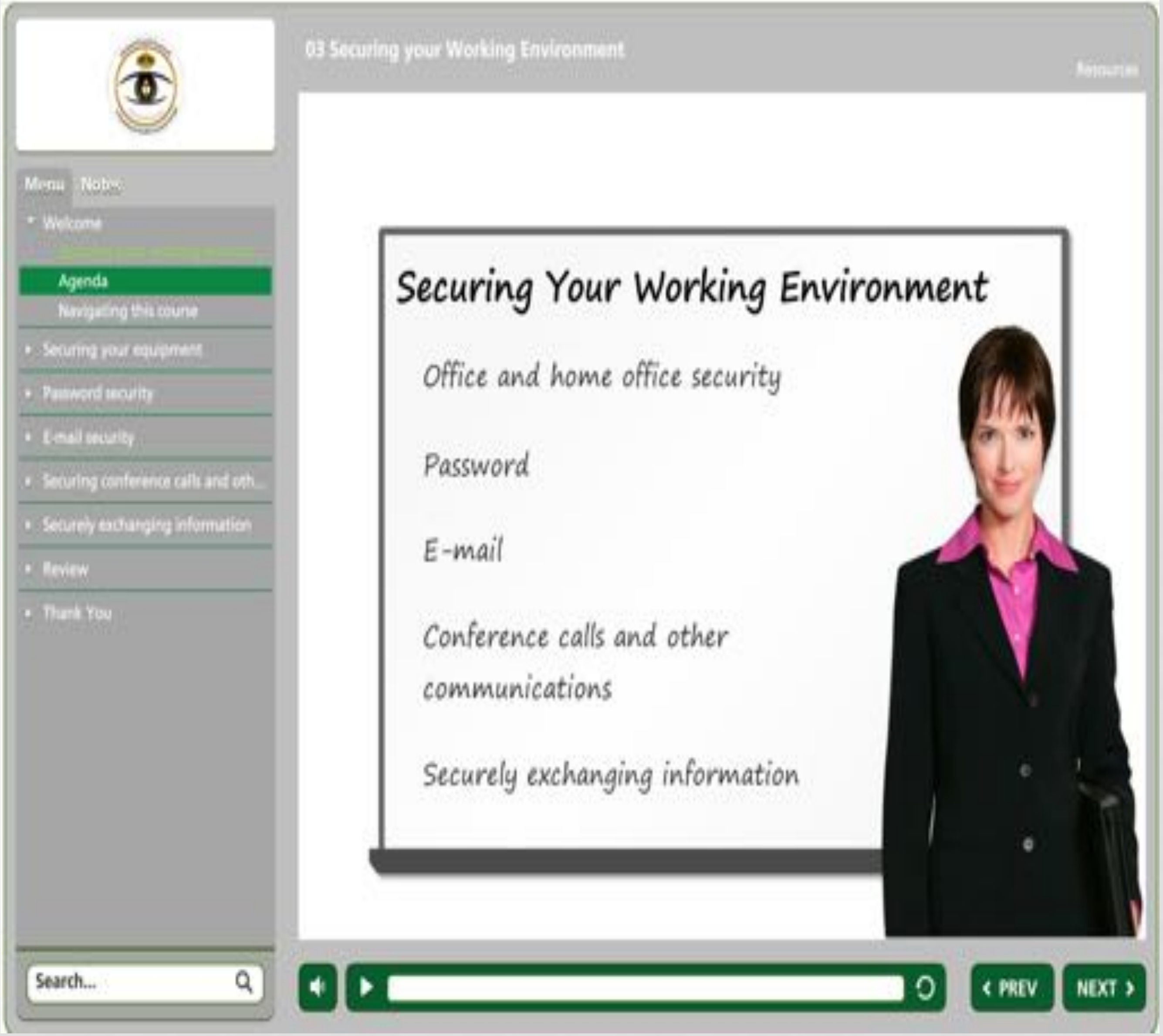
Introduction to Information Security



The Clean Desk Principle

Learning Activity

Look at the following image and select the items that compromise information security by not complying with the Clean Desk Principle.



03 Securing your Working Environment

Securing Your Working Environment

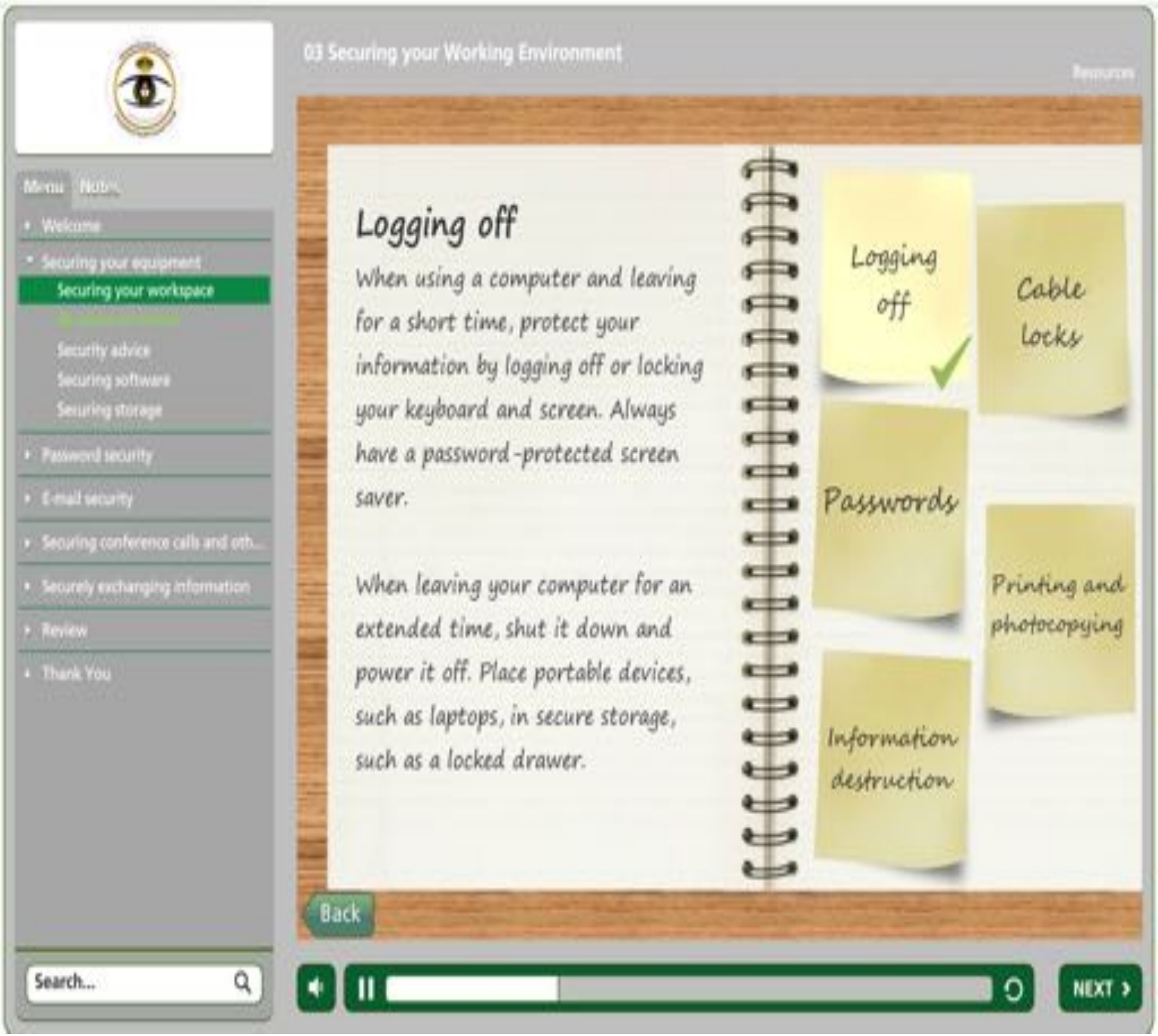
Office and home office security

Password

E-mail

Conference calls and other communications

Securely exchanging information



Logging off

When using a computer and leaving for a short time, protect your information by logging off or locking your keyboard and screen. Always have a password-protected screen saver.

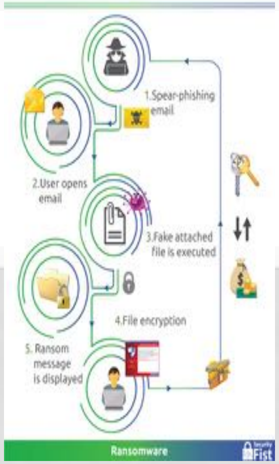
When leaving your computer for an extended time, shut it down and power it off. Place portable devices, such as laptops, in secure storage, such as a locked drawer.

REMINDERS / MARKETING TOOLS

REMINDER TOOLS

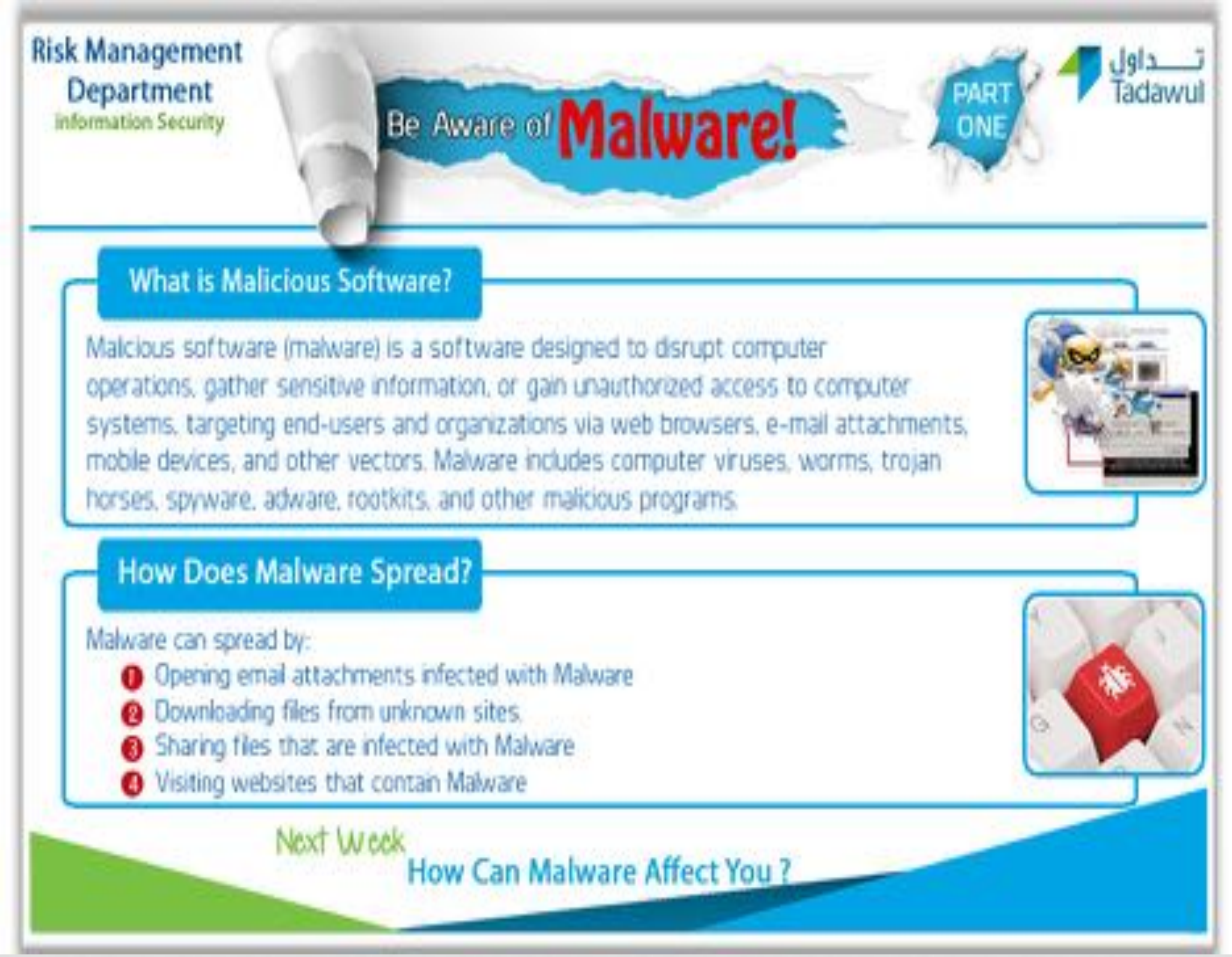
- Posters
- Screen Savers
- Flyers
- Mugs
- USB Drive
- Pen
- Key Chains

Hard To Ignore Facts About Passwords
75%
Of people use the same password for multiple accounts
48%
Of people have shared a password with someone else
One in six admits accessing someone else's account by guessing their password.
Most popular passwords are 'password' and 123456
40%
Of users do not bother with complex passwords or fail to change their passwords on regular basis
90%
Of employee passwords can be cracked within 6 hours.
SecurityFist



The 10 most dangerous practices at work
Using unencrypted external devices in storing important and sensitive data
Using the same username and password for different accounts
Sharing personal passwords with others
Keeping confidential data on your personal device
Connecting to unsecure wifi
Using personal mobile devices to connect to the organization's Wi-Fi
Carrying a device containing sensitive data during travel with no purpose
Not watching for shoulder surfers while handling confidential data
Not reporting to your organization when losing an external device containing confidential and sensitive data
Leaving your PC unlocked while you are away
SecurityFist

SAMPLES – EMAIL MESSAGES



Risk Management Department
Information Security

Be Aware of **Malware!**

PART ONE

تــــداول
Tadawul

What is Malicious Software?

Malicious software (malware) is a software designed to disrupt computer operations, gather sensitive information, or gain unauthorized access to computer systems, targeting end-users and organizations via web browsers, e-mail attachments, mobile devices, and other vectors. Malware includes computer viruses, worms, trojan horses, spyware, adware, rootkits, and other malicious programs.

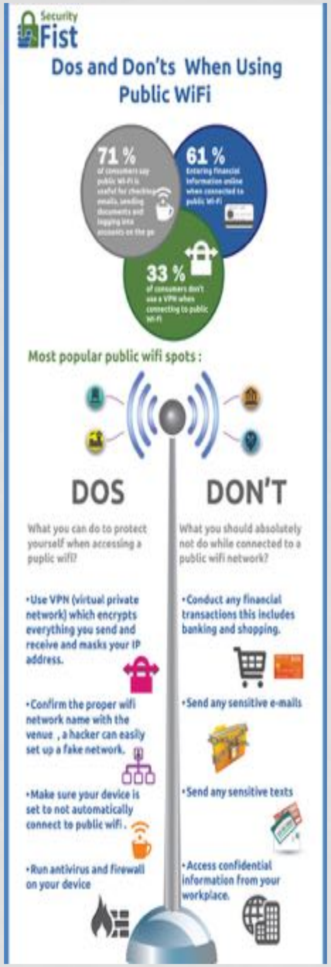
How Does Malware Spread?

Malware can spread by:

1. Opening email attachments infected with Malware
2. Downloading files from unknown sites.
3. Sharing files that are infected with Malware
4. Visiting websites that contain Malware

Next Week
How Can Malware Affect You ?

SAMPLES - POSTERS



Security Fist

Dos and Don'ts When Using Public WiFi

71 % of consumers say public Wi-Fi is useful for checking emails, sending documents and logging into accounts on the go

61 % Entering financial information online when connected to public Wi-Fi

33 % of consumers don't use a VPN when connecting to public wi-fi

Most popular public wifi spots :

DOS

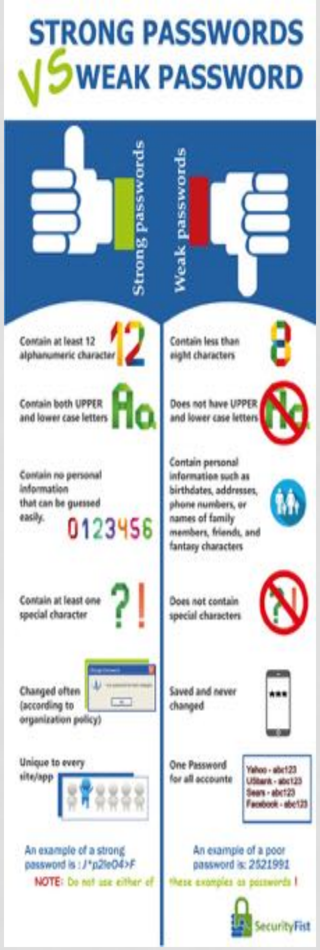
What you can do to protect yourself when accessing a puplic wifi?

- Use VPN (virtual private network) which encrypts everything you send and receive and masks your IP address.
- Confirm the proper wifi network name with the venue , a hacker can easily set up a fake network.
- Make sure your device is set to not automatically connect to public wifi .
- Run antivirus and firewall on your device

DON'T

What you should absolutely not do while connected to a public wifi network?

- Conduct any financial transactions this includes banking and shopping.
- Send any sensitive e-mails
- Send any sensitive texts
- Access confidential information from your workplace.



STRONG PASSWORDS VS WEAK PASSWORD

Strong passwords	Weak passwords
Contain at least 12 alphanumeric character	Contain less than eight characters
Contain both UPPER and lower case letters	Does not have UPPER and lower case letters
Contain no personal information that can be guessed easily.	Contain personal information such as birthdates, addresses, phone numbers, or names of family members, friends, and fantasy characters
Contain at least one special character	Does not contain special characters
Changed often (according to organization policy)	Saved and never changed
Unique to every site/app	One Password for all accounte

Yahoo - abc123
USbank - abc123
Sears - abc123
Facebook - abc123

An example of a strong password is : J*p2le04>F

An example of a poor password is: 2521991

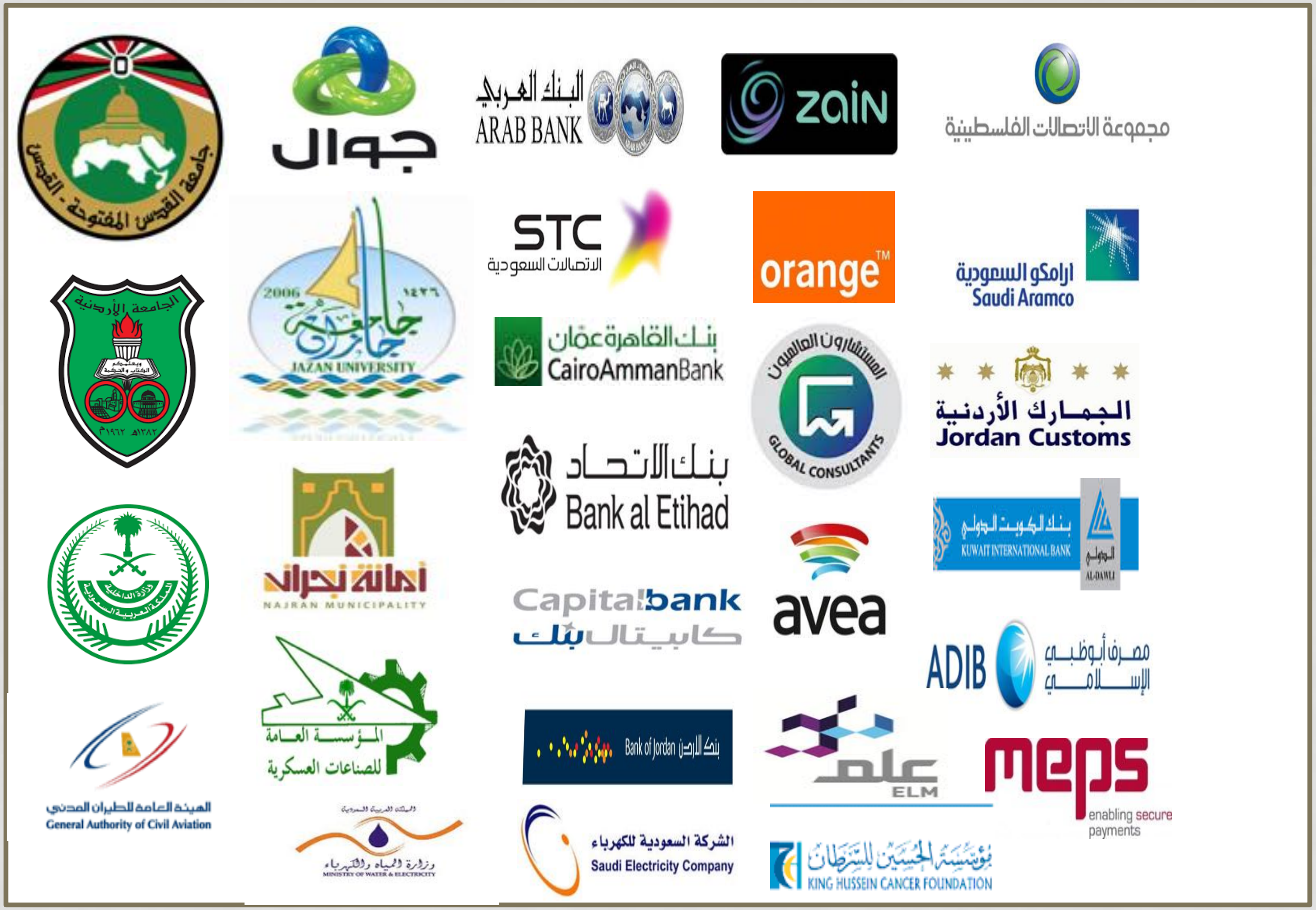
NOTE: Do not use either of these examples as passwords !

SecurityFist

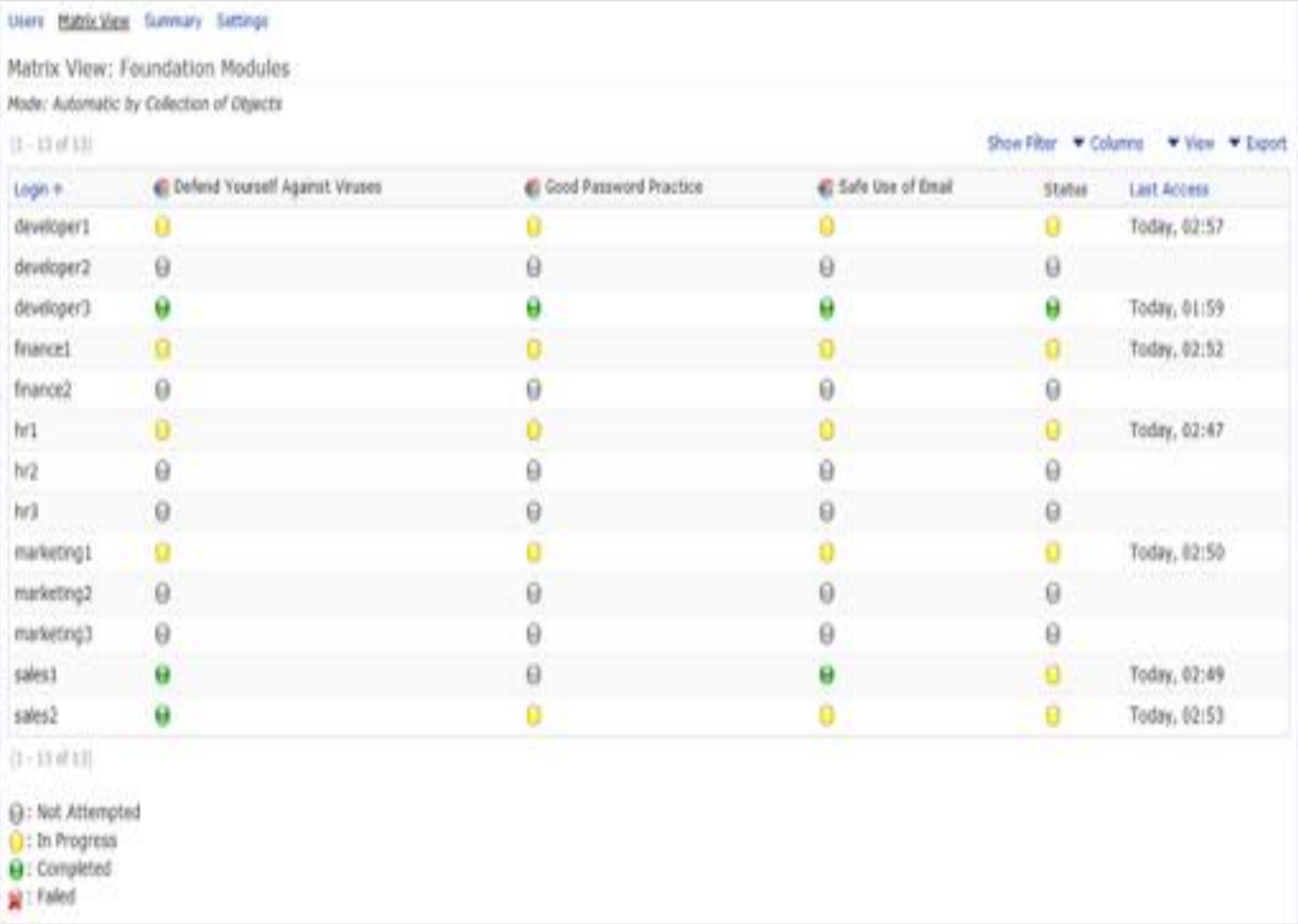
SAMPLES – CALENDARS

Protect Your Password
Using symbols, numbers and capital letters in your password will significantly increase it's strength.
IT SECURITY
www.itsecurityct.com
Protect Your Password
March

SAMPLE CUSTOMER LIST



REPORT: STAFF PROGRESS



Matrix View: Foundation Modules

Mode: Automatic by Collection of Objects

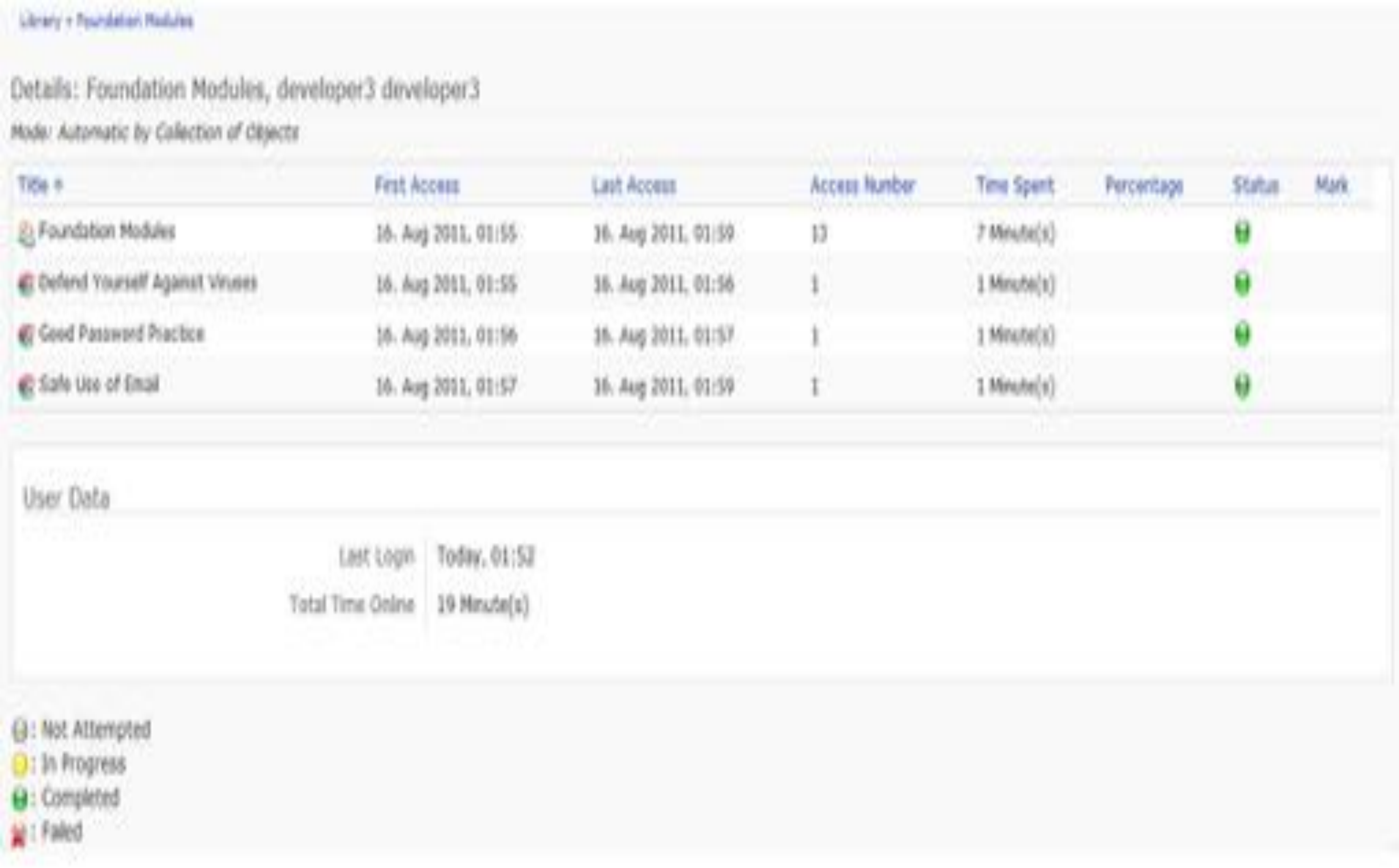
[1 - 13 of 13]

Login +	Defend Yourself Against Viruses	Good Password Practice	Safe Use of Email	Status	Last Access
developer1	🟡	🟡	🟡	🟡	Today, 02:57
developer2	⚪	⚪	⚪	⚪	
developer3	🟢	🟢	🟢	🟢	Today, 01:59
finance1	🟡	🟡	🟡	🟡	Today, 02:52
finance2	⚪	⚪	⚪	⚪	
hr1	🟡	🟡	🟡	🟡	Today, 02:47
hr2	⚪	⚪	⚪	⚪	
hr3	⚪	⚪	⚪	⚪	
marketng1	🟡	🟡	🟡	🟡	Today, 02:50
marketng2	⚪	⚪	⚪	⚪	
marketng3	⚪	⚪	⚪	⚪	
sales1	🟢	⚪	🟢	🟡	Today, 02:49
sales2	🟢	🟡	🟡	🟡	Today, 02:53

[1 - 13 of 13]

⚪ : Not Attempted
🟡 : In Progress
🟢 : Completed
❌ : Failed

REPORT: INDIVIDUAL



Library » Foundation Modules

Details: Foundation Modules, developer3 developer3

Mode: Automatic by Collection of Objects

Title ↓	First Access	Last Access	Access Number	Time Spent	Percentage	Status	Mark
Foundation Modules	16. Aug 2011, 01:55	16. Aug 2011, 01:59	13	7 Minute(s)		🟢	
Defend Yourself Against Viruses	16. Aug 2011, 01:55	16. Aug 2011, 01:56	1	1 Minute(s)		🟢	
Good Password Practice	16. Aug 2011, 01:56	16. Aug 2011, 01:57	1	1 Minute(s)		🟢	
Safe Use of Email	16. Aug 2011, 01:57	16. Aug 2011, 01:59	1	1 Minute(s)		🟢	

User Data

Last Login	Today, 01:52
Total Time Online	19 Minute(s)

○ : Not Attempted

🟡 : In Progress

🟢 : Completed

✗ : Failed

CERTIFICATE

A customized certificate could be issued to confirm users' attendance and passing of the end of course quiz

Certificate of Completion

This certifies that

Has successfully completed the

This ___ Day of ______ ____

Signature

Certificate

letion

Certifies that

Has Completed the

Security Awareness: Social Engineering

IT Security Consulting and Training LLC