Cyber and Data Security Training Courses 2016

Overview

01905 317173 | @FriendlyNerdUK | www.friendlynerd.co.uk

The Friendly Nerd Limited, Wyche Innovation Centre, Walwyn Road, Malvern, Worcestershire, WR13 6PL

CYBER BASICS (HALF-DAY)

Learning objectives

- To provide a basic foundation of cyber security knowledge for general staff within a company or organisation
- To enable attendees to understand the key concepts of cyber security and how they apply to their own day-to-day activities
- To raise awareness of the impact of cyber incidents and the reasons why they occur.
- To provide basic advice good practice to prevent cyber incidents from an end-user perspective.

Course description

This course is aimed at all staff within a company and provides basic guidance and advice on how to look after a company's data and prevent cyber incidents from occurring.

The course would fit well as part of an organisation's security awareness programme and can be customised to comply with the security policy of a particular organisation.

Course structure

Part 1 – What is cyber security?

- Groups involved and methods used
- Impact of cyber incidents

Part 2 – Cyber Basics – how to keep secure day-to-day

- Passwords
- Phishing and social engineering
- Secure configuration
- Anti-virus and malware
- Wi-Fi and mobile working
- Updates and patches

Part 3 – Scenarios

- Short scenarios where attendees apply their learning to typical day-to-day situations

Target audience

The course assumes a generalist and non-technical audience. No prior experience or knowledge of cyber security is required.

Price

£850 for up to 20 people

DATA PROTECTION IN ACTION (HALF-DAY)

Learning objectives

- To enable attendees to understand key concepts of the data protection act and how to apply them to their own organisation.
- To provide background and understanding of the principles of data protection
- To provide practical advice on how to deal with determining purpose, Subject Access requests, data retention and data auditing.
- To assist attendees to understand the impact of data breaches and provide basic advice on how to help keep company and personal data safe through good practice
- To understand the changes to Data Protection legislation coming into effect with the EU General Data Protection Regulation

Course description

This half-day course provides the knowledge needed to understand the basics of data protection within an organisation. It is appropriate for anyone who comes into day-to-day contact with personal or sensitive data within an organisation and provides a foundation of knowledge to enable data to be handled appropriately. It would also be suitable to managers and leaders who wish to implement good practice within an organisation.

The course is a mix of formal training and a short interactive exercise where attendees are encouraged to apply their learning in a number of scenarios.

Course structure

Part 1 – Why Data Protection?

- What are we seeking to protect and why
- Principles of data protection
- Key terms and their meaning
- What happens when data protection goes wrong?
- Changes to come from European-wide legislation

Part 2 – Data protection principles in practice

- Identifying purpose
- Identifying personal data within your work area
- Subject access requests
- Data retention and classification
- How to keep data safe – data security basics
- Dealing with incidents

Part 3 – Scenarios

- Short scenarios where attendees apply their learning to example situations

Target audience

The course assumes a generalist audience. No prior knowledge of data protection is required.

Price

£850 for up to 20 people

STRATEGIC CYBER SECURITY FOR DECISION MAKERS (FULL-DAY)

Learning objectives

- To enable managers and leadership teams to make decisions on how to change an organisations business processes to reduce the risk of cyber incidents
- To enable attendees to understand the key ideas of risk, data security and the essential technical controls that enable cyber security
- To assist the development of a cyber security strategy and information security policy for an organisation
- To provide a background on how to develop a security awareness campaign for staff and how to deal with cyber incidents

Course description

This course provides simple, practical advice on the steps that should be taken to prevent cyber incidents within an organisation from a strategic and operational perspective. The course is appropriate for managers, leaders and decision makers across business areas. It would also suit those who are part of an advisory board and need to set strategic direction.

The course is a mix of formal training and a short interactive exercise where attendees are encouraged to apply their learning in a number of scenarios.

Course structure

Part 1 – What is cyber security?

- Groups involved and methods used
- Impact of cyber incidents on organisation

Part 2 – A strategic approach to cyber security

- How to set a strategic direction on cyber security
- How to assess and measure cyber risks
- Creating an information security policy and legislation

Part 3 – Operational measures to decrease risk

- How to identify and categorise your data
- Developing security awareness and good practice in staff
- Key technical measures to prevent cyber incidents
- Certifying your information security compliance

Part 4 – Scenarios

- Short group scenarios on the above to enable attendees to apply their learning

Target audience

The course covers cyber security topics at a leadership/strategic level and assumes candidates have a working knowledge of their organisation, the types of data held and activities carried out. Detailed knowledge or experience of cyber security is not required.

Price

£1,200 for up to 20 people

DEVELOPING SECURITY AWARENESS (HALF-DAY)

Learning objectives

- To enable HR managers, IT managers and leaders to develop a data security culture within their organisation through a security awareness programme
- To enable attendees to understand the elements that make a successful security awareness programme and to be able to apply these to their own organisation
- To enable attendees to understand the key concepts of cyber security and the basic security messages their programmes should provide to their staff

Course description

The course takes you through the process of developing your own security awareness campaign within your organisation, including:

- How to decide on appropriate security messages and how to relate to policy
- How to get the message across (methods to use, frequency of messages, focus on staff joiners/leavers)
- How to target messages to different audiences(office staff, warehouse staff, finance, suppliers, contractors)
- How to measure impact

The course would be well suited to HR managers, IT managers and department heads, or anyone who has a remit to develop security awareness across an organisation.

Course structure

Part 1 – What is cyber security?

- Brief overview of cyber security and the role staff play to keep data secure

Part 2 – Developing a data security culture within your organisation

- Messaging – what are you trying to communicate?
- How to relate to company policy – do you need to create a policy?
- Who are your audience and why?
- What methods can be used to communicate
- Which are most cost-effective
- Ongoing messages versus event-timed messages (joiners/leavers/contractors)
- Linking the programme to training – basic cyber skills for staff
- Measuring impact – what can be measured?

Part 3 – Scenarios

- Short scenarios where attendees apply their learning to their own organisation

Target audience

The course assumes a non-technical audience. No prior experience or knowledge of cyber security is required.

Price

£850 for up to 20 people