CORPORATE TRUST
business risk & crisis management

How to be security-conscious online

GOAL:

The risk of a virus, Trojan horse, or other types of malware finding their way onto your PC as a result of surfing the net is growing constantly. More than ever, criminals are setting out to exploit people's incautious behavior as a way of accessing confidential data or to set up what are known as "botnets" by infecting several thousand computers. Barely a day goes by without a report of companies having their data stolen or bank account holders falling victim to phishing expeditions seeking to discover their PIN or TAN. The formats which these attacks take are becoming ever more sophisticated, with hackers frequently turning Internet users' carelessness against them.

Nowadays, criminals can use confidential data to easily forge identities or generate passwords. The necessary information can be found on social networking profiles such as Facebook or XING, with further details being cleverly extracted over the phone (by means of "social engineering"). The faked identities can then be used to order goods over the internet, from eBay or Amazon, for example, or to attack a company network via a supposedly authorized password.

How can I protect myself against viruses, Trojan horses, or drive-by downloads? How can social engineering techniques be recognized at the earliest stage? What is the best way to conduct myself on social networking sites? If you do not yet know the answers to these and similar questions, you should take this opportunity to find out.

The training on how to be security-conscious online offered by Corporate Trust teaches you about all currently known forms of such attacks, as well as the ways in which you can protect yourself against them. Besides becoming aware of how to recognize social engineering techniques, you will find out what optional settings will protect you against information theft on social networking sites and how you can recognize critical online attacks.

For children and young people, we offer training sessions which are specially adapted to their typical patterns of behavior, such as use of online games, chat rooms, etc.

TARGET AUDIENCE:

- People who use the Internet in a business setting
- Private individuals
- Children and young adults

RESULTS:

By becoming aware of the risks associated with the internet, how you can safeguard against them, and what privacy settings you should use on social networking sites, you can protect your own personal data and your company's expertise.

TRAINERS:

The Corporate Trust trainers leading these sessions have many years of practical experience in combating computer crime and industrial espionage.

CONTENT AND AGENDA:

1. Current forms of attack using viruses, Trojan horses, and other malware

2. Typical patterns of behavior of cybercriminals:
   - Social engineering
   - Phishing
   - Identity theft

3. Protective measures when surfing the Net:
   - Anti-virus programs & firewalls
   - How to deal with e-mails
   - Browser settings

4. Social networking sites:
   - Privacy settings
   - Recognizing critical attempts to make contact
   - Settings for photos and personal data
   - Links to other services

5. Emergency measures in the event of:
   - A suspected infected PC
   - Identity theft, phishing, etc.

DURATION:

2 – 3 hours

SESSION LOCATION:

The training is held on your premises.

PRICE:

€ 2,000

CONTACT:

For further information or a specific quote, please contact:

Christian Schaaf
Managing Director
Phone: +49 (0)89 599 88 75 80
schaaf@corporate-trust.de