
Be Security Aware!
How to protect
Your company
Your family
Yourself
InfoSecurityLab

- Part 1. *General information*
- Part 2. *Kinds of threats*
- Part 3. *Information security*
- Part 4. *Ways of treatment*
- Part 5. *Participation*
- Part 6. *Latest methods of deceit*
- Part 7. *How to deal with them*
- Part 8. *Some more instructions*

Part 1

General information

We all hate taking security measures...

- Remembering passwords
- Locking doors & computers
- Cryptographic protection

InfoSecurityLab

Today's world

A world with *global sharing information.*

But this has pros and cons...

PROS

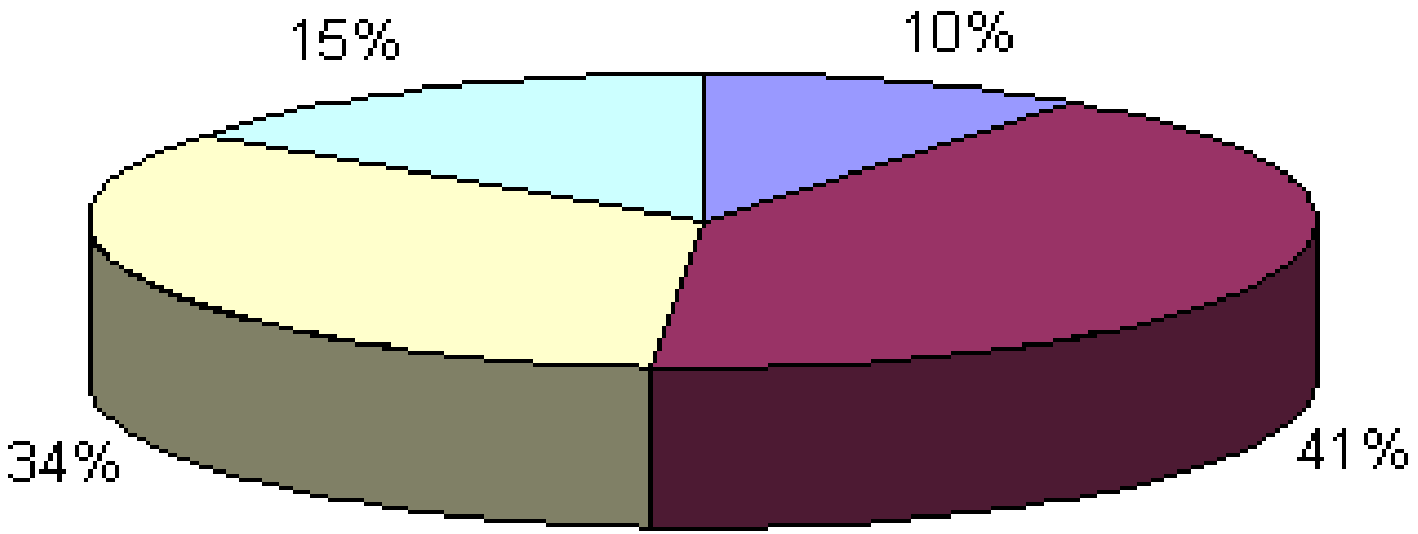
- Internet gates
- Freedom in communication
- Exchange of information
- Quick sharing of files
- Open connection to the whole world

CONS

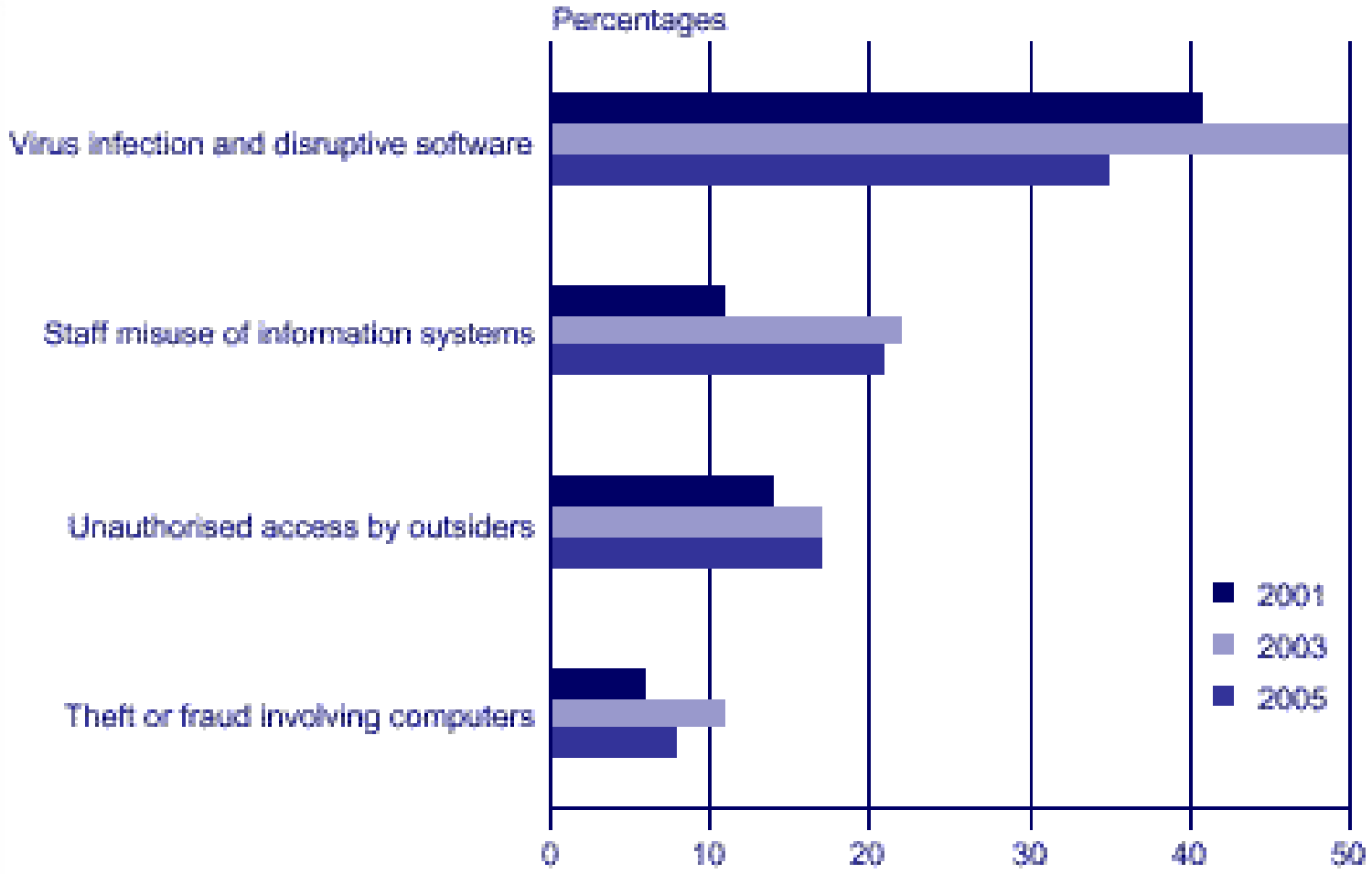
- Loss of control in privacy
- Threats in information resources
- Confidentiality in danger

Some statistics...

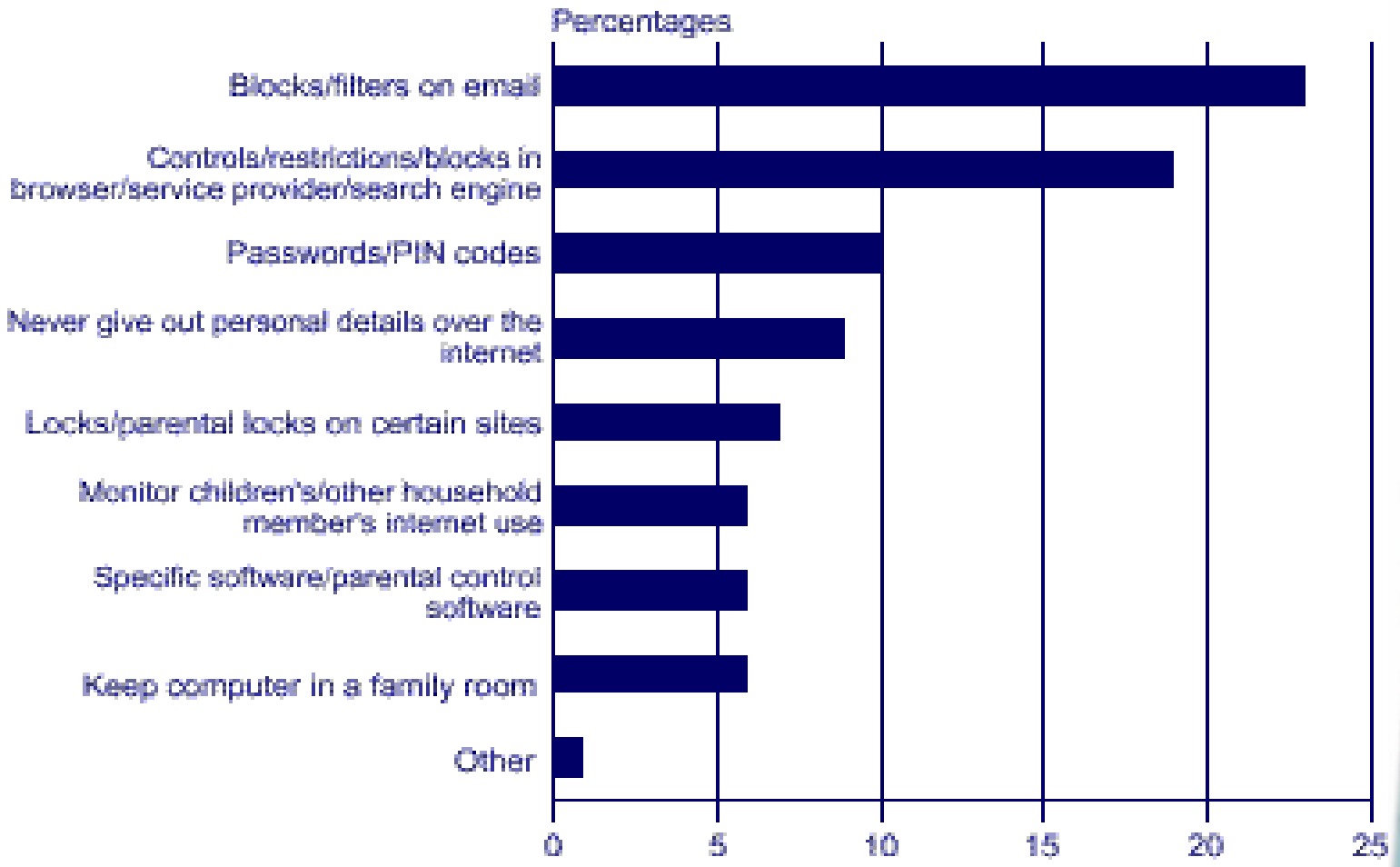
Attacks & Abuses



Source: http://www.statistics.gov.uk



Source: www.cubic-labs.com



Source: www.cubic-labs.com

Need for security awareness

- Competition in business
- Sensitive personal data
- Confront the danger of losing money
- Protect children from internet threats

How to do it...?

A COMPLETE & DETAILED TUTORIAL IS A MAJOR COMPONENT OF ANY AWARENESS TRAINING PROGRAM

Part 2

Kinds of threats

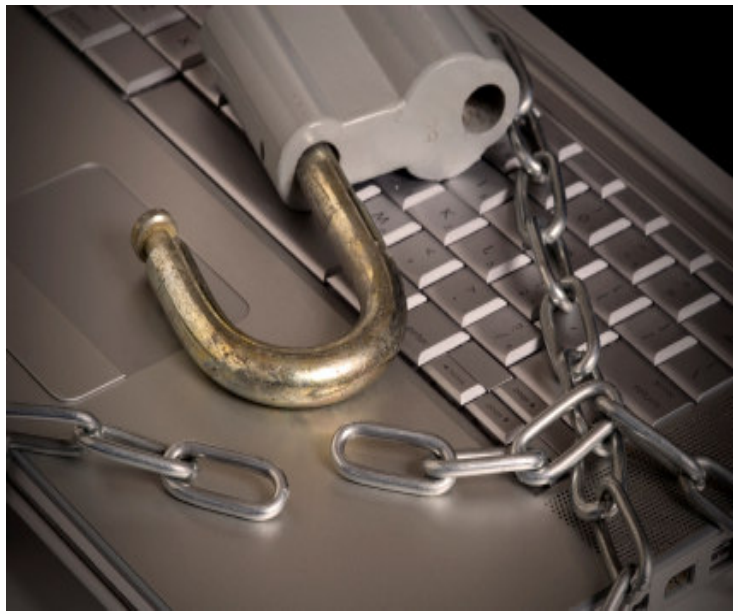
A pile of threats...

...that want to invade our privacy

worms

Computer programmes that harm the whole network, not just a single computer!

hackers



A person with a great knowledge of computer technology, who may try to harm your files and steal your identity.

spyware

Computer software that collects the personal information of the users, without their approval.

trojan horses

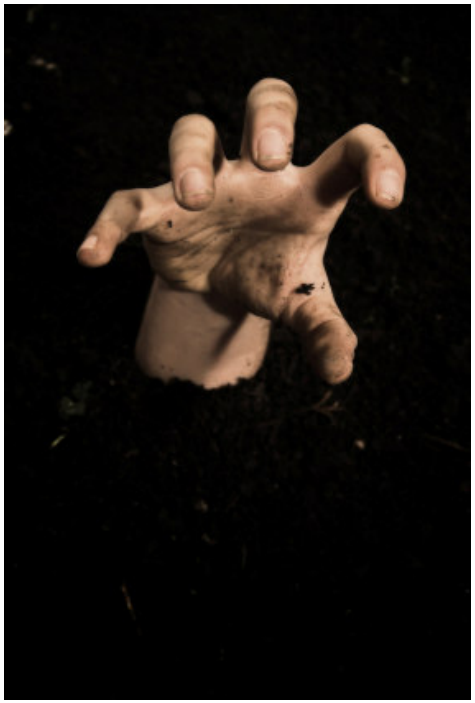
A programme, extremely harmful when executed, that depends on the victim's actions. It masquerades as something else, in order to trick the user.

viruses

A computer programme that copies itself and infects more computers, without the permission of their users.

InfoSecurityLab

zombies



A computer set online by a hacker, a virus or a trojan horse, so as to perform malicious tasks under remote control.

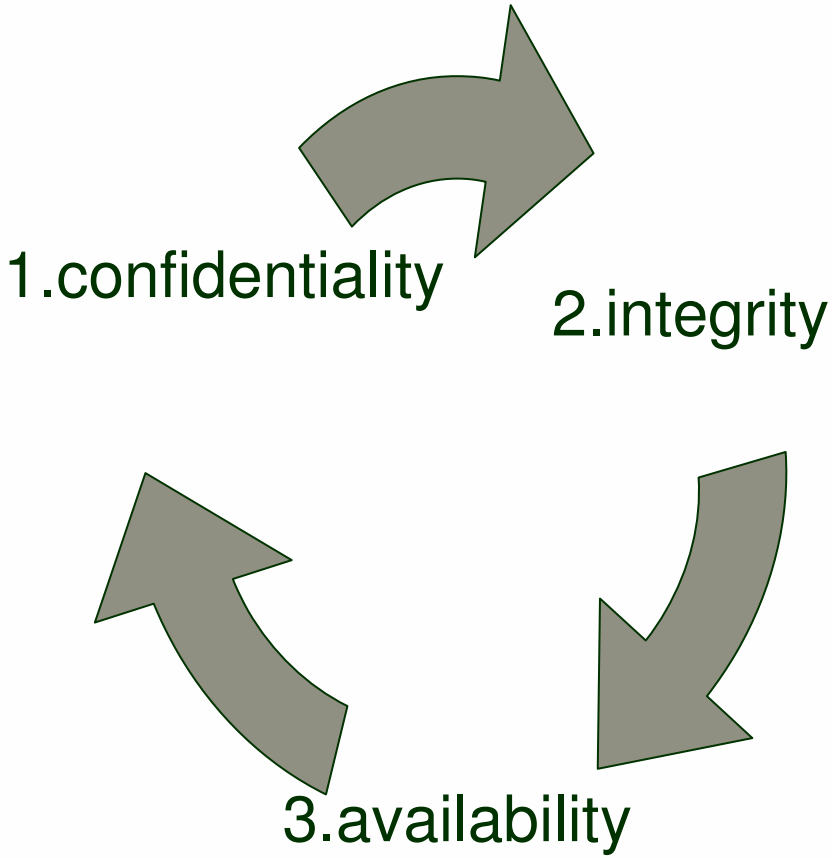
phishing

Way of acquiring sensitive information through e-communication, by disorientating the victim.

Part 3

Information security

The 3 pillars of information security



1. Confidentiality

Confidentiality means that data can be accessed only by authorized users, and if abused, can cost a lot of money!

2. Integrity

Integrity means that data can be modified only by authorized users, and if not, it can be expensive too! (salaries, strictly secret files, etc)

3. Availability

Availability means that all data should be accessible when authorized people need it!

Company's culture 1

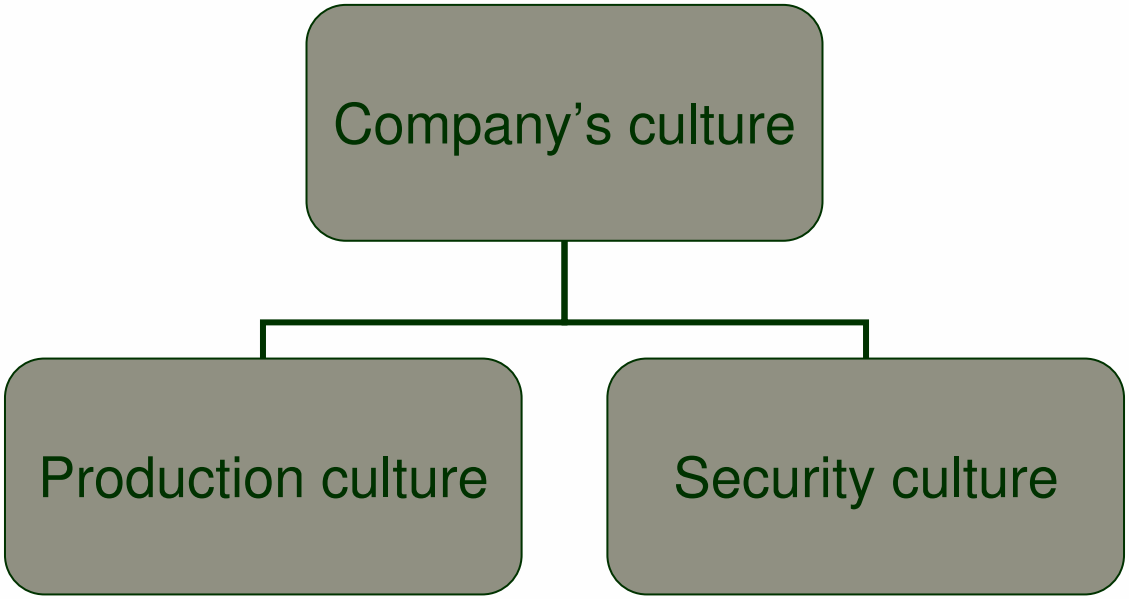
- A culture is the values and polices which are adopted by the whole labour force of a company.
- Company's culture is important because it is usually adaptively aligned to the business goals, and can lead to an outperformance of its competitors.
- Company's culture evolves and changes over time, but the stronger it is, the less it will be influenced by new employees joining the business, new products, new laws, new regulations, etc.

Company's culture 2

- It also changes a little while becoming mature from a startup to a more established company. Major or minor changes can be positive or negative.

- It is up to a manager's will to determine a desired company's culture, and through this support every little sub-culture exists, although it could be controversial.

Production Culture VS Security Culture



Production Culture

- production is what matters
- the corporate value is to get the job done
- security performance is not taken under account
- security is not the supervisor’s job

Security Culture

- security is a basic team value
- security performance is always measured & tied to daily action
- security is integrated into all operations of the company

How to combine these controversial elements...

The company has to invest in a dynamic awareness program, which has to conform with the company's production spirit. Security concerns everyone.

Part 4

Ways of treatment

Steps to be followed

1. Security awareness culture survey
2. Detect danger signs
3. Security planning
4. Crisis management
5. Change behaviors

1. Strategic content sessions

AIM: **TO SPOT THE EXISTING SECURITY WEAKNESSES**

- *Incident reports*
- *Compliance measuring tools*
- *Tests (online, hard copies)*
- *Interviews with supervisors*
- *Oral & written surveys by employees*

2. Identifying the problem

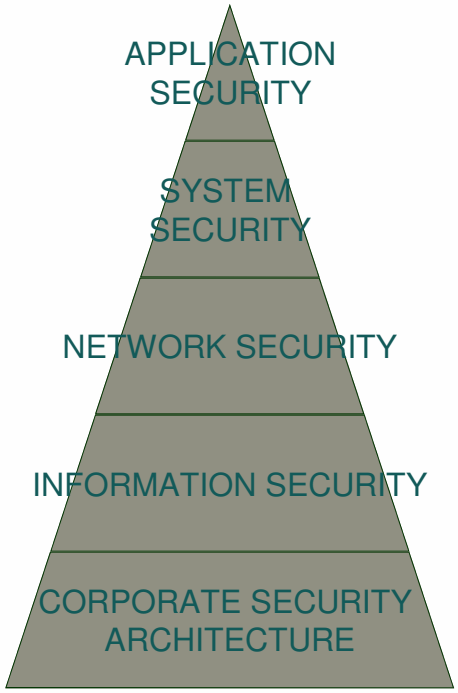
THROUGH TESTS & DETAILED INTERNAL RESEARCH

The risk level depends on the existing information :

- *Public*
- *Internal use*
- *Confidential*
- *Restricted*

We've got to specify the needs of each target group & then spread the message.

3. Security planning



- assess security requirements
- develop information security policies
- implement policies through processes and procedures
- enable security architecture through auditing and testing
- update policies based on changing business needs and technologies

4. Crisis management

The inevitable happens...All necessary measures have to be taken due to any possible attack. Any information leak has to be confronted, without interrupting the normal flow of services. Every employee has to be informed about security issues and the management has to promote risk reduction in every way, on a daily basis.

Crisis management involves:

- Information back up
- Secure copies of all data
- Instead of panic reactions in a crisis, employees will follow the guidelines
- There is a well structured business continuity plan
- Employees are all aware of the person who is authorised to start the emergency procedures
- Everyone must know and exercise their role in the emergency procedures
- Public relations contacts are regulated in order to protect the company's reputation

5. Change in behavior

People adopt new patterns of behavior when the old are no longer effective. Providing them with knowledge doesn't guarantee this change. Their involvement in the whole security project is a major factor. Team work is required.

Part 5

Participation

Involvement

Employees want to have a feeling of involvement in the whole project of security awareness.

How do you achieve that?

- Security promotion weeks
- Security newsletters
- Increase interest in protection
- Clean desk practice at the end of each workday
- Security champions awards

You just have to take personally all these threats online and:

- Involve yourself in any march of events, around security awareness.
- Discuss security matters, even during lunch break.
- Suggest new safety practices to your manager.

Need for team work

- The seeds of awareness must be sown to everyone.
- Each person should know the relevance of security to their job.
- A company should invest in the human resource first, so as not to pay later for the security mistakes.
- Everyone has to learn how to apply security in the context of their work.
- Find ways to attract all stakeholders in security discussions and activities.
- Security is not just the responsibility of the executive and management team.

TECHNOLOGY COMES AND GOES...PEOPLE WILL ALWAYS BE THE CHALLENGE!

Security concerns everyone!

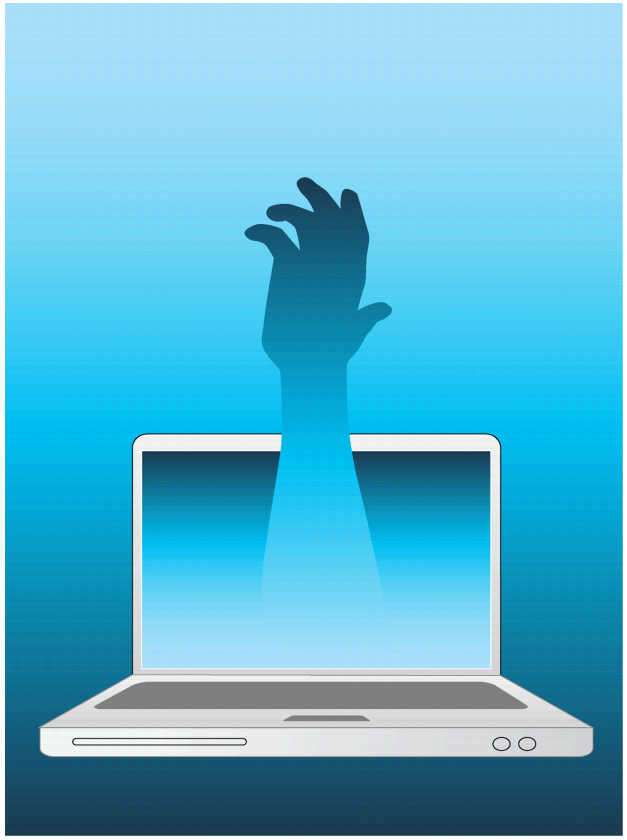
Together we can keep safe...

InfoSecurityLab

Part 6

Latest methods of deceipt

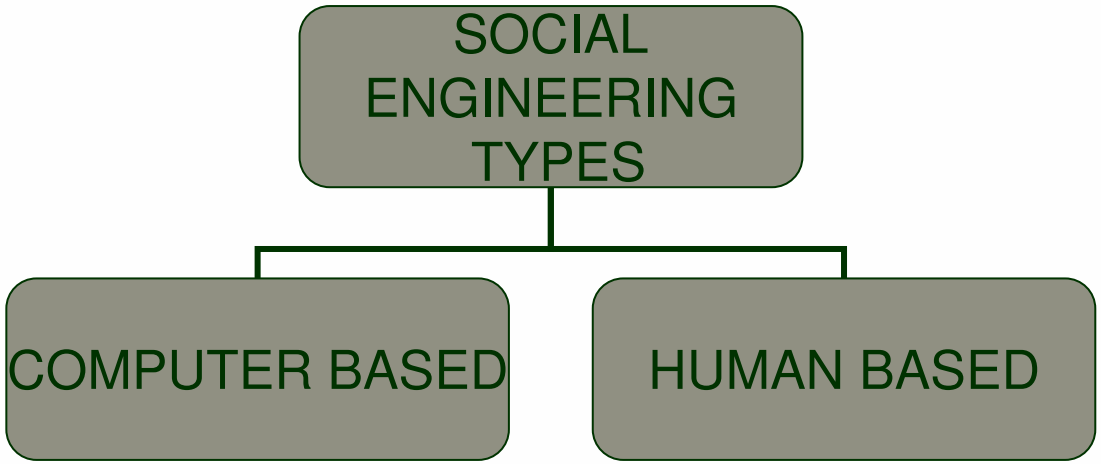
Social Engineering



InfoSecurityLab

- Social Engineering is a kind of security attack in which someone manipulates others into revealing information.

- Social Engineers usually chisel confidential data out of employees by relying on people's tendency to trust people and to avoid getting into trouble.



- **Computer based attacks:** a computer software is used, so as to convince employees to reveal the desired information.

- **Human based attacks:** person-to-person interplay, so as to convince employees to reveal the desired information.

Social engineering techniques

- Impersonation
- Flattery
- Trusted relations
- Sense of urgency
- Popup windows
- Mail attachments
- Chain letters
- Spams
- Third-party authorization

Common dialogues

- -Hello, this is Mr Jones from technical support. There was an attack in your account. I have to rectify the error immediately. I need some details Sir, because the whole system is in danger.

  -Yes, of course.

  -What is your password? I need to save the computer files.

  -It's my surname, Clark.

  -Thank you, I will keep you informed for this inconvenience.

- -Hello, can I talk to Mr Jones please?

  -I'm sorry he's out of the office.

  -Who am I talking to?

  -His coleague, Clark.

  -Well, Mr Clark, he told me that you would have sent me the new designs by noon and it's 3 o'clock! Weren't you informed? I'm Mr Smith!

  -No, I'm sorry.

  -My fax is 0679043, forward them to me quickly. We will lose the client!

  -Ok, I'm so sorry for this delay.

Part 7

How to deal with them

Watch your moves!

Some important things to have in mind...

Beware of what's on your
desk, in your trash and
generally clean the whole workplace.

Never write down your password,

never type it while someone can observe your keyboard.

InfoSecurityLab

Don’t talk loudly about private information.

InfoSecurityLab

Don’t reveal privileged communication by e-mail or phone conversations.

Always ask your supervisor if something looks suspicious.

Role play scenarios

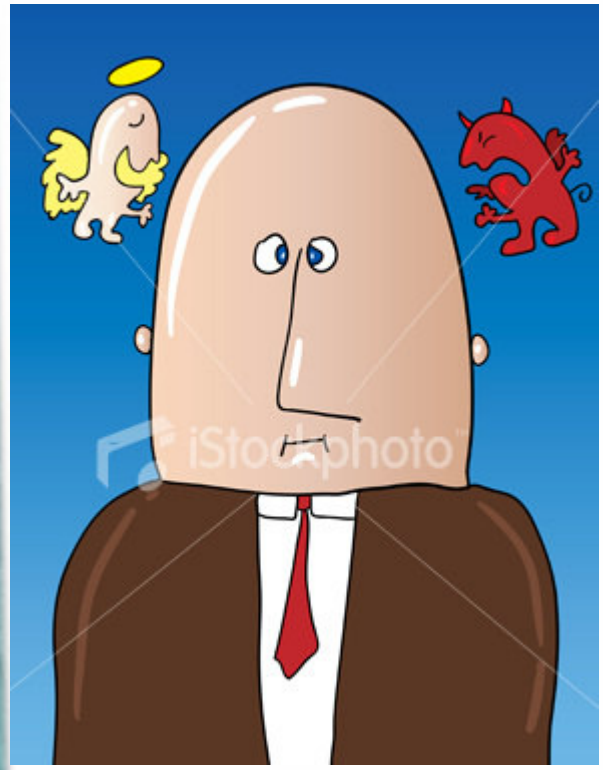
IT'S AN EFFICIENT WAY OF TEACHING EMPLOYEES ABOUT SECURITY MEASURES THAT CAN BE TAKEN, WHILE WORKING, AGAINST DATA THEFT, SOCIAL ENGINEERING, VIRUSES, ETC.

This kind of experimental learning promotes good practice in information security and ensures that it is applied effectively across the enterprise.

Scenario 1

You noticed some people entering your work place, without wearing an identity badge. Think of how you need to react in an imaginary dialogue with them.

Scenario 2



You receive a call from someone who seems aware of many confidential files in your computer. He asks you for information, you are not sure you should share with someone. What will you do?

InfoSecurityLab

Scenario 3

How will you react if you receive an email,where you are informed about a security break and you will be asked to change your password to a new one, proposed by the system administration?

Part 8

Some more instructions

Be prepared for any malfunction that could happen all of a sudden, and which could have, as a result, a big loss – of information or money.

InfoSecurityLab

Try to be prepared so as to remain calm in any crisis situation.

Don’t trust anyone who enters your workplace.

InfoSecurityLab

Rehearse what you've learned by trying to test the readiness of your colleagues.

Imaginary dialogues between you and social engineers can be helpful when you need them for real!

Things to have in mind

- It's not only about company's files, but people's lives too.
- Knowing all the existing dangers, keeps you safe.
- Knowledge never goes for nothing!

So remember…

Amateurs Hack Your Systems
Professionals Hack You

Don't let them intrude into your life... Secure the entrance.

Be aware!

InfoSecurityLab