ISSeG

Computer Security Advice for users

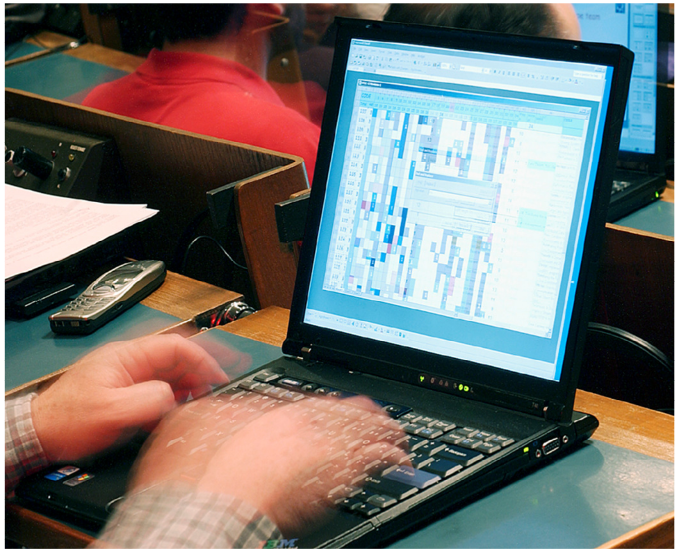
Integrated
Site
Security for
Grids

See: http://www.isseg.eu/training

Information Society and Media

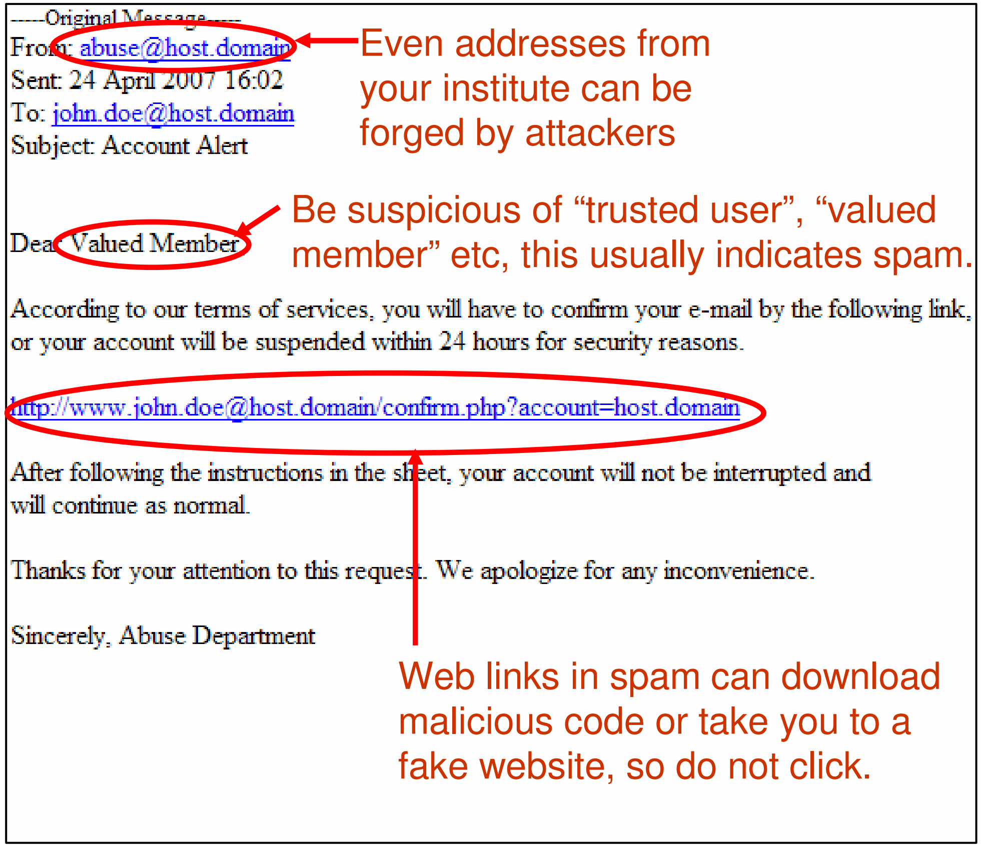
What causes most incidents?

- **Many incidents are due to a lack of security awareness**
- **You need to know the information in the following slides, which will cover:**
  - Tricks attackers use
  - Web links and pop-ups
  - Installing software
  - Screen locking
  - Passwords



Be aware of tricks attackers use

- **Attackers use tricks to get you to infect your own computer:**
  - Curiosity (‘look at this’, empty mail, …)
  - Trust (from a friend, colleague, …)
  - Authority (from security, management, …)
- **Do not click on web links in spam and unexpected emails, instant messages and chat**
- **Do not open attachments that you are not expecting**



-----Original Message-----
From: abuse@host.domain
Sent: 24 April 2007 16:02
To: john.doe@host.domain
Subject: Account Alert

Dear Valued Member

According to our terms of services, you will have to confirm your e-mail by the following link, or your account will be suspended within 24 hours for security reasons.

http://www.john.doe@host.domain/confirm.php?account=host.domain

After following the instructions in the sheet, your account will not be interrupted and will continue as normal.

Thanks for your attention to this request. We apologize for any inconvenience.

Sincerely, Abuse Department

Even addresses from your institute can be forged by attackers

Be suspicious of “trusted user”, “valued member” etc, this usually indicates spam.

Web links in spam can download malicious code or take you to a fake website, so do not click.

An example of a fake email

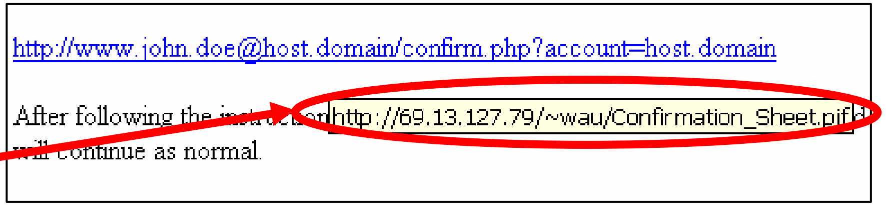
Integrated
Site
Security for
Grids

Be suspicious of web links and pop-ups

- **“Fake” web links in emails, instant messages and chat can link to a different web site than expected**

- **Some web links and pop-ups can automatically download malicious software, so think before you click**

- **With some pop-ups, even clicking “Cancel” or “No” or closing the window with the top-right “X” can still infect your machine**
  - On a Windows PC, close a potentially malicious pop-up by pressing the keys [Alt][F4], which closes the “active” window



http://www.john.doe@host.domain/confirm.php?account=host.domain

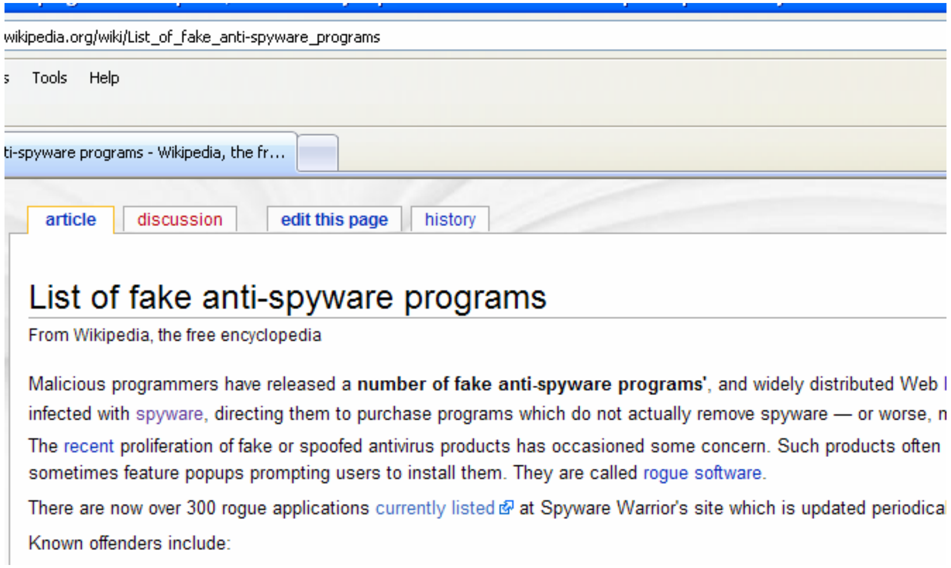
After following the instruction http://69.13.127.79/~wau/Confirmation_Sheet.pif will continue as normal.

By hovering your mouse over a web link WITHOUT CLICKING you reveal its real destination.
If in doubt, don’t click the link

Integrated
Site
Security for
Grids

Avoid installing additional software

- **“Free” versions of software may contain Trojan horses, spyware or other malicious software that could infect a PC**


wikipedia.org/wiki/List_of_fake_anti-spyware_programs

List of fake anti-spyware programs

From Wikipedia, the free encyclopedia

Malicious programmers have released a **number of fake anti-spyware programs'**, and widely distributed Web I
infected with spyware, directing them to purchase programs which do not actually remove spyware — or worse, n

The recent proliferation of fake or spoofed antivirus products has occasioned some concern. Such products often sometimes feature popups prompting users to install them. They are called rogue software.

There are now over 300 rogue applications currently listed at Spyware Warrior's site which is updated periodica

Known offenders include:

Some quick online research can often help identify malicious software

- **Plug-ins may also contain malicious software**

If a website requires a plug-in to view it, try to avoid using it

Integrated Site Security for Grids

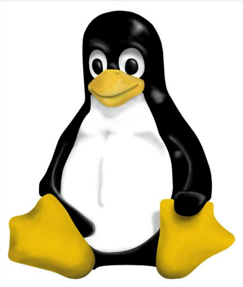
See: http://www.isseg.eu/training

Information Society and Media

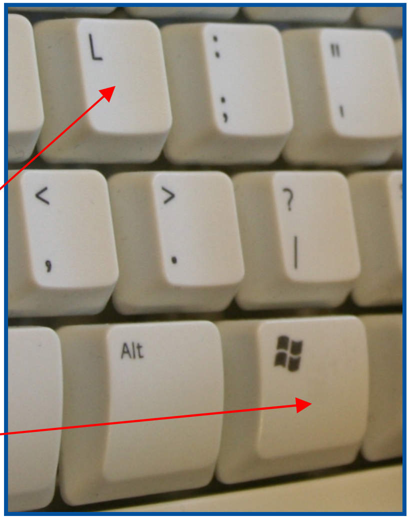
Lock screen when leaving your office

- **Locking your screen prevents others accessing confidential material**

  - From a **Linux** desktop, verify that the screen saver is enabled and configured to lock the screen



  - From a **Windows** PC use [Control][Alt][Delete] and select “Lock Computer”
    - Or if you have a Windows keyboard, simply press [Windows][L]



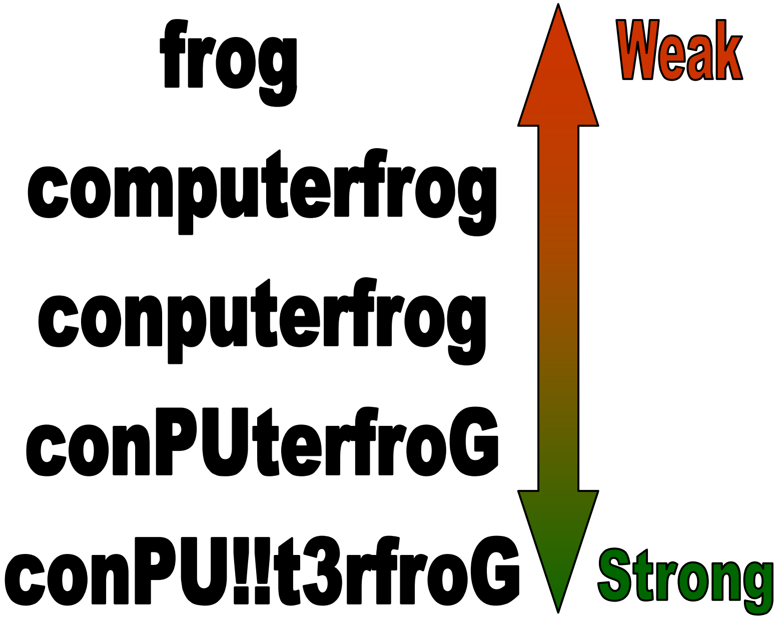
Integrated Site Security for Grids

See: http://www.isseg.eu/training

Information Society and Media

Do not expose your password

- **Never use your institute passwords for private use**
- **Never tell someone your password**
  - Not even support staff or requests by phone
  - Be wary of emails, instant messages and chat requesting your password often via web links
- **If you think your password may have been exposed, change it and notify your IT support team**



A strong password should be at least 8 characters long and a mixture of at least 3 of the following: upper case letters, lower case letters, digits and punctuation

ISSeG

For additional security information and advice, visit http://www.isseg.eu/training