

Internet Segura na Escola

Mestre Luís Costa

Departamento de Ciências e Tecnologias

Universidade Autónoma de Lisboa

Tópicos

A Universidade no centro de Lisboa

- ▶ **A Segurança na Comunicação**
- ▶ **Perigos da Internet**
- ▶ **Proteger os alunos**
- ▶ **Conclusões**

A Segurança na Comunicação

A Universidade no centro de Lisboa

Internet, Comunicação e Segurança

- ▶ A Internet é uma fonte e uma via de **comunicação**
- ▶ A comunicação **nunca é** totalmente segura
- ▶ Conclusão: é indispensável estar atento à **insegurança** quando se utiliza a Internet

Perigos da Internet

A Universidade no centro de Lisboa

Perigos da Internet

- ▶ Invasão de vírus, worms e ligações com sítios (*sites*) inseguros
- ▶ Instalação de programas “piratas”
- ▶ Fornecer dados pessoais próprios e da família (*phishing* – p.ex. formulários para confirmar dados) que podem ser usados abusivamente
- ▶ Demasiada dispersão de actividades e perda de tempo útil ao estudo

Perigos da Internet

- ▶ Contactos com gente desconhecida que pode ser origem de diversos danos sociais (desvio de menores, convites para actos ilícitos)
- ▶ Contacto com sítios que promovam racismo, uso de armas e consumo de droga
- ▶ Formas de acesso:
 - * Salas de bate-papo (*chat*)
 - * *E-mail*, incluindo *spam*
 - * *Blogs*
 - * *Telefones celulares, principalmente com acesso à Internet*

Perigos da Internet

- ▶ Mensagens de pessoas que não se conhece
- ▶ Pedidos de dados pessoais de desconhecidos
- ▶ Encontros com pessoas desconhecidas com base em contactos apenas através da Internet
- ▶ Sofrer agressões pela Internet
- ▶ Propostas sexuais agressivas ou duvidosas

Perigos da Internet

- ▶ Passar informações pessoais para pessoas que não se conhece com segurança
- ▶ Falta de cuidados familiares (ignoram o que os filhos fazem na Internet)
- ▶ Alguns pais nunca discutem com os filhos os problemas de segurança na Internet

Perigos: conclusão

Os 5 “C”

- ▶ **C**onteúdos → impróprios, ilegais, inadequados)
- ▶ **C**ontactos mal intencionados
- ▶ **C**omércio enganoso e sem ética
- ▶ **C**omportamentos irresponsáveis e compulsivos (forte dependência da Internet)
- ▶ **C**opyrighth → violação de direitos de autor, devido a cópias não autorizadas

Proteger os alunos

Proteger: o que se pode fazer

- ▶ Continuar a falar abertamente sobre os computadores em família e em aula
 - * Amigos
 - * Jogos
 - * Conversas
 - * Partilha de informações

Proteger: o que se pode fazer

- ▶ Ter os computadores numa área aberta e não no quarto das crianças
- ▶ Ensinar a colocar na Internet apenas informação que qualquer pessoa possa ver
- ▶ Ensinar a montar e a usar procedimentos de segurança

Proteger: o que se pode fazer

- ▶ Ensinar a não falar com estranhos
- ▶ Relembrar o não dar informação pessoal (número de BI, endereço, telefone, escola, turma, etc)
- ▶ Estabelecer regras em casa e na escola para se usar a Internet

Proteger: o que se pode fazer

- ▶ Ter conversas frequentes sobre os perigos e a forma de evitá-los
- ▶ Lembrar as consequências positivas e negativas das redes sociais

Proteger: o que se pode fazer

- ▶ Fazer um **contrato** com os alunos que devem **assiná-lo**
 - * Indicando o que podem e não podem fazer na Internet
 - * Enfatizar a importância de não dar nenhuma informação a desconhecidos
 - * Especificar orientações de comunicação com outros pela rede
 - * Estabelecer penalizações (ex: suspensão do uso), que devem ser cumpridas

Proteger: o que se pode fazer

- ▶ Instalar programas de restrição de acesso por URLs e por conteúdo
- ▶ Abrir os computadores em aula apenas quando for necessário à aula e com ordem do professor
- ▶ Estabelecimento de limites de horários
- ▶ Examinar periodicamente
 - * O histórico de acesso dos utilizadores
 - * Dispositivos de armazenamento usados pelos alunos (CDs, DVDs, *pen drives*, etc.)

Proteger: o que se pode fazer

- ▶ Verificar se a escola
 - * Tem política de segurança de uso da Internet pelos alunos
 - * Promove uma cultura de segurança a ser seguida por professores e alunos
 - * Instalou programas de protecção nas redes

Proteger: o que se pode fazer

- ▶ Ter em atenção os truques usados por crianças e jovens para enganarem o controlo de pais e professores
 - * Criam várias contas de *e-mail*
 - * Usam ferramentas de *chat*
 - * Criam páginas pessoais em sítios grátis
 - * Instalam browsers diferentes do usado normalmente
 - * Mudam o nome do arquivo do programa

Proteger: o que se pode fazer

Instalação de dois tipos de programas

- ▶ 1. Controlo de acesso
- ▶ 2. Monitorar o uso

Proteger: o que se pode fazer

1. Controle de acesso

- ▶ CyberPatrol da SurfControl
 - * Bloqueia conteúdos inapropriados
 - * Bloqueia serviços indesejados, como chat
 - * Diferentes perfis podem ser definidos para cada membro da família
 - * Já vem com filtros pré-configurados para diferentes idades

Proteger: o que se pode fazer

2. Monitorar o uso

▶ PC Tattletale

- * Usa poucos recursos
- * Não se nota a sua montagem → crianças não percebem que está instalado
- * Activado por meio de Ctrl+Alt+alguma tecla ou na janela de comandos (*prompt*)
- * Grava todas as actividades feitas com a Internet

Conclusões

A Internet na formação da Pessoa

- ▶ A Internet existe → tem **benefícios** de informação e tem **perigos** que dependem muito da acção das escolas e das famílias
- ▶ Todo o processo educativo deve ter uma **orientação** para que produza efeitos benéficos

A Internet na formação da Pessoa

- ▶ A escola, o professor podem orientar as crianças e os adolescentes a utilizar a Internet para **fins úteis à sua formação**
- ▶ E também podem ensiná-los a **distinguir** o que pode ser perigoso do que é confiável

Alguns programas apropriados para filtrar informação não desejada

- ▶ [http://weblocker.fameleads.com/
get_weblocker.asp](http://weblocker.fameleads.com/get_weblocker.asp)
- ▶ <http://pt.terrasoft.com.br>
- ▶ <http://www.cyberpatrol.com>

