APUNTAMENTOS DA CHARLA SOBRE SEGURIDADE INFORMÁTICA

IES de Chapela, 15 de maio de 2012

Poñente: Luís Alberto Luaces Bustabad

REDES SOCIAIS

A seguridade nas Redes Sociais é 0. Cuns pequenos coñecementos calquera persoa pode entrar en todos os datos do perfil e modificalos.

PROBLEMAS:

- **Pederastas** acceden a datos e poden facerse pasar por outras persoas para concertar unha cita (Houbo 3 agresións en Vigo no último ano).
- As **fotos** que se suban son **incontrolables**, aínda que logo se volvan baixar. Nunca podemos subir fotos de terceiras persoas sen o seu consentimento. En Vigo creouse un perfil con foto roubada. O perfil foi insultado e a fotografada DENUNCIOU POR INXURIAS. O xulgado de menores amoestou aos menores causantes, que quedaron con antecedentes penais, e púxolle multa de 6000€ aos pais.

Programas Peer-to-Peer (P2P)

EXEMPLOS: Ares, eMule, BitTorrent, Napster, eDonkey.

Son legais. Serven para intercambiar calquera tipo de arquivos informáticos. Nos arquivos suxeitos a propiedade intelectual **non se persigue a copia privada**. É **delito se se vende ou se dona**, xulgándose no xulgado do penal cunha pena de ata 2 anos de prisión.

PROBLEMAS:

- Perigo de infección por **virus** informático e por **intrusións**. Porque para usar os programas P2P hai que abrir os cortalumes do ordenador.

Pornografía infantil

É **delito TER un arquivo**, e pode ser xulgado polo penal con penas de ata 1 ano de prisión.

Descargar un único arquivo xa é delito, porque queda rexistrada a descarga, aínda que despois o eliminemos.

Se por erro descargamos un destes arquivos **debemos** poñernos en contacto coa Policía.

Navegación por internet

Hai 3 tipos de páxinas:

- **htpps**: Páxinas Seguras. Non son invulnerables pero si dan seguridade.
- **Fiables**: Porque son de **empresas coñecidas** que se farían cargo do que me pase.
- **Non fiables**. O resto.

PRÁCTICAS NOCIVAS:

- H**OAX** (bulos): estratexias para que o usuario faga o que quere o delincuente (por exemplo escribir o teléfono, ou o correo electrónico ou calquera dato persoal).
- **PHISHING**: Enganan ao usuario poñendo falsas páxinas de bancos e piden nº de conta bancaria, ou piden enviar contrasinal do correo electrónico.
- **PHARMING**: Troiano que redirecciona a páxinas falsas de bancos para quedarse con contrasinal e nº de conta.
- **MALWARE**: (Adware ou spyware) é un virus que controla as webcams. Recoméndase ter o obxectivo tapado.
- **MÁQUINA ZOMBIE**: Control remoto de ordenadores para almacenar neles SPAM, Pornografía, etc

Consellos na navegación por Internet

- Non aportar **nunca datos persoais.**
- Desconfiar das páxinas de **subastas** (eBay) que poden se unha **estafa** na que se piden anticipos con escusas.
- Non contactar con descoñecidos (poden ser depredadores sexuais ou pederastas)
- Non mentir nas redes sociais para maiores de 13 porque desprotexen legalmente ao menor.
- Non fiarse nada das **mentiras de internet** (anorexia, sectas ....)
- Apagar a Wi-Fi cando non se usa.
- Actualizar o Sistema Operativo regularmente.
- Ter instalado un Antivirus bo que se actualice a diario.
- Facer copias de seguridade en dispositivos non conectados a internet.
- Ter un contrasinal de calidade, con letras, números e outros carácteres.
- Nunca introducir datos persoais en Internet.

Algúns apuntamentos lexislativos

- Non existen delitos específicos de internet. Habitualmente as denuncias son por inxurias (falar mal de alguén) ou ameazas.
- O uso da Wi-Fi dun veciño non é delito.