UNIDADE 15

Cybercrime

- ✓ Você já foi vítima de algum crime virtual ou conhece alguém que tenha caído em algum golpe na Internet?
- ✓ Você sabe como são as leis no Brasil em relação a este tipo de crime?
- ✓ O que é necessário para se proteger dos crimes virtuais?

EXERCÍCIO 1: Veja a lista de crimes virtuais abaixo e faça o que se pede a seguir:

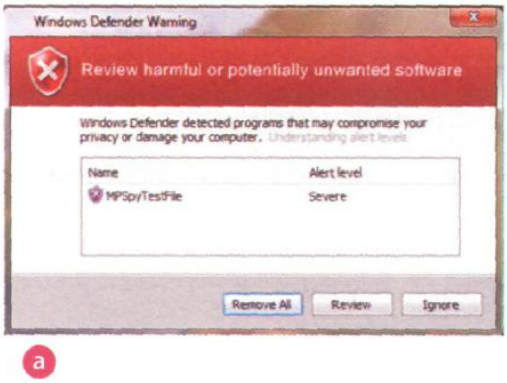
Cybercrimes

- **Piracy** – the illegal copy and distribution of copyrighted software, games or music files
- **Plagiarism** and **theft of intellectual property** – pretending that someone else's work is your own
- **Spreading of malicious software**
- **Phishing** (password harvesting fishing) – getting passwords for online bank accounts or credit card numbers by using emails that look like they are from real organizations, but are in fact fake; people believe the message is from their bank and send their security details
- **IP spoofing** – making one computer look like another in order to gain unauthorized access
- **Cyberstalking** – online harassment or abuse, mainly in chat rooms or newsgroups
- **Distribution of indecent or offensive material**

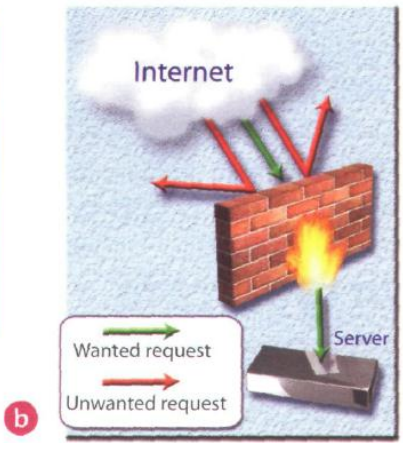
a) Which crimes are most dangerous?
b) Is it fair or unfair to pay for the books, songs or videos you download?
c) Personal information are stored in database by marketing companies. Is our privacy in danger?

EXERCÍCIO 2: Faça a correspondência dos textos com as imagens:

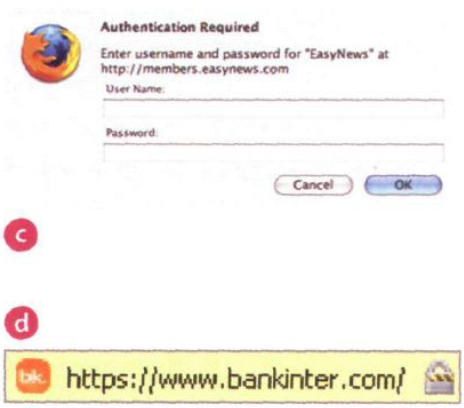
1) A secure website can be recognized in two ways: the address bar show the letters HTTPS and a closed padlock or key is displayed at the bottom of the screen.
2) You have to type your username and password to access a locked computer system
3) This program displays a message when it detects spyware and other unwanted software that may compromise your privacy and damage your work.
4) Private networks use a software and/or hardware mechanism to block unauthorized traffic from the internet.



a



b



c
d

EXERCÍCIO 1: Após ler o texto, responda as perguntas abaixo:

Cybercrime is biggest UK fear

Warwick Ashford

ComputerWeekly.com

Cybertheft is the UK's most feared crime, outranking burglary, assault and robbery according to a study of more than 1,400 regular internet users by Tickbox.net.

The research, commissioned by security software makers AVG, reveals that 43% of Britons feel most vulnerable to cybertheft compared with burglary (29%), assault (18%) and robbery (11%). About one in three people in the study had been affected by some form of cybertheft over the internet including fraudulent e-mails, credit card fraud, and unauthorised bank transfers. Amounts taken ranged from just a few pounds to several thousand pounds.

The survey shows that financial transactions over the internet are on the rise with 85% of people using the internet for shopping and over two-thirds doing their banking online, but as many as 87% admitted they were worried about the threat of cybertheft. Although 90% said they had some form of threat protection on their computer, 33% said they were not convinced they had adequate measures in place to protect themselves. Just 3% said they used no protection at all, but 25% said there was not enough information available on cybertheft to then to protect themselves adequately. Liverpool is the city most afraid of cybertheft with 93% citing it as a concern, followed by Glasgow with 92% and Cardiff third with 91%.

"While the risks of theft over the internet are real, it is important to keep it in perspective," said Larry Bridwell, global security strategist at AVG.

He said there were a number of things that could be done, such as installing internet security software and updating it regularly, using only industry-recognised internet-payment systems, and checking that payment sites are secure by looking for the padlock symbol on the screen.

a) Após os crimes virtuais, quais crimes são mais temidos na Inglaterra?

_____

b) O segundo parágrafo mostra que:
- O medo das pessoas está fazendo com que elas comprem menos pela Internet.
- As transações online aumentam, assim como o medo de comprar pela internet.
- As compras virtuais aumentam e a maior parte dos entrevistados tem medo de fazer compras pela Internet.

c) A frase "While the risks of theft over the internet are real, it is important to keep it in perspective" significa:
- É preciso ter uma perspectiva do que são os riscos na Internet.
- É importante considerar os riscos da Internet ao utilizá-la.
- Os roubos via Internet mostram uma nova perspectiva para a indústria de softwares.

Leia rapidamente os textos A e B e faça o que se pede a seguir.

A Computer security

Picter den Bieman, a legal practitioner specialising in information technology, is speaking at a Chamber of Commerce lunch.

'I'm sure you'd all agree that the development of information technology and e-commerce has presented exciting business opportunities. However, the increasing sophistication of the systems and applications available to **end users** has created significant **legal challenges** to individuals, companies, the legislature, and legal advisers. The technology necessary to access the Internet has also enabled **innovative illegal activities**. You'll be aware that these include the **breach of computer security** and **unauthorised access** to a computer commonly known as **hacking**. There's also the distribution of **illegally obtained content** from databases, as well as **virus writing** or **virus spreading** achieved by attacks on **insecure servers** which lack adequate protection. In the UK, the **Computer Misuse** Act deals with such illegal use, and also the publication and distribution of material that may be used to aid hacking. Unfortunately, unless you have **adequate security systems** in place, your business is at risk.'

Exercício 2: Verifique se as afirmações abaixo são verdadeiras (V) ou falsas (F), baseando-se no texto A:

a) People who use computer applications are known as hackers.
b) It's a legal challenge to gain unauthorized access to a database.
c) Secure servers make virus spreading possible.
d) Distributing illegally obtained data is a breach of computer security.

Exercício 3: Baseado no texto B, complete as lacunas do artigo do The Times abaixo:

B Cybercrime

'There are **cybercrimes** that may affect you personally, such as credit card fraud online, commonly known as **credit card scams**, and **identity (ID) theft**, when **financial benefit** is **obtained by deception** using stolen personal information. In the USA, **fraudsters**, as they're known, who use a **stolen identity** to commit new crimes, may be charged with what's known in the States as **aggravated ID theft**. The Council of Europe Cybercrime Treaty, also signed by US and Japan, has the aim of international co-operation and **mutual assistance in policing**.

Other cybercrime may impact on your business. There's **cyberfraud**, such as **pharming**, where users are moved to **fake**, non-genuine sites, when they try to link to their **bona fide** bank website. Then there's **phishing**, when a fraudster, by **misrepresentation**, gets Internet users to **disclose personal information** in reply to spam email sent unsolicited to a large number of people. Internet users can also be tricked into **money laundering** activities which aid the transfer of illegal or stolen money.'

Pharming is taking over from phishing

International cyber-crooks have found a new way to rip off the public

Fraudsters find it surprisingly easy to operate credit card (1) ..... over the Internet. (2) ..... tricks consumers into providing confidential details in response to spam email. Although banks have been raising public awareness of the practice by placing warnings on websites, some customers are still taken in by spam emails inviting them to (3) ..... account information.

But phishing is no longer as effective as it was, so (4) ..... have developed (5) ..... , which does not involve spam email and is harder to detect. The scam redirects users to (6) ..... sites when they try to access their (7) .... bank website. A customer logs on, normally using the address stored in his or her 'favourites' folder, to what looks like the bank's internet banking site, but the customer is actually redirected to the fraudster's site.

The fraud is no longer limited to bank accounts. Recent examples have had corporate websites cloned to sell non-existent products, or to get consumers to participate in money (8) ..... activities while believing they are dealing with a legitimate organisation.

Whether the fraudsters are using phishing or pharming, criminal prosecution remains difficult, largely because most of the criminals are based outside the territory in which the victim resides. Extradition proceedings are difficult and rare, although some national courts may have limited extra-territorial jurisdiction. Phishing legislation may be drafted but the real problem is the cross-border nature of the fraud. The legislation may have no teeth, leaving the perpetrators almost immune from prosecution.

The Times

Exercício 5: Veja a tabela abaixo publicada no relatório UK Cybercrime Report 2009:

Category	2008	2007	2006	Change 07/08
Identity theft and identity fraud	86,900	84,700	92,000	+2.6%
Financial fraud	207,700	203,700[3]	207,000	+1.9%
Online harassment	2,374,000	2,240,000	1,944,000	+6.0%
Computer misuse (excluding viruses)	137,600	132,800	144,500	+3.6%
Sexual offences	609,700	617,500[4]	850,000	-1.3%
Total	**3,415,900**	**3,278,700**	**3,237,500**	4.2%

a) Em primeiro lugar, diga qual categorias de crimes teve maior aumento no período pesquisado e qual teve menor incidência.

b) Dê exemplos de crimes que podem estar incluídos em cada uma dessas cinco categorias:

CRIME	EXEMPLOS
ID theft and ID fraud	
Financial fraud	
Online harassment	
Computer misuse	
Sexual offences	

Exercício 5: A Revista Forbes listou as maiores condenações por crimes virtuais em 2008. Em primeiro lugar, leia os títulos e diga sobre o que cada um deles deverá tratar. Em seguida, fale sobre cada uma delas.

Phishing Spam

The federal CAN-SPAM Act, passed back in 2003, makes it illegal to send unsolicited e-mail without an opt-out function or with misleading header or subject information. The first criminal prosecutions under the law are only now starting to trickle into the federal system. Jeffrey Brett Goodin of Azusa, Calif., has the dubious distinction of being the first felon convicted under this law, according to the Department of Justice. He was sentenced in June 2007 to five years and 10 months in federal prison for sending thousands of phishing e-mails to AOL customers, asking them to update their credit card information on fraudulent Web pages, and then using their financial details to commit identity theft.

Pornographic Spam

Jeffrey Kilbride of Venice, Calif., and James Schaffer of Paradise Valley, Ariz., tried mixing racy photos into millions of spam e-mails that they sent out, hoping to drive recipients to a series of porn sites. The result? First, more than $1 million in revenue--then a variety of obscenity charges added to their violations of the CAN-SPAM Act. In October, Kilbride was sentenced to 72 months in prison. Schaffer received 63 months.

Stock Spam

Aside from phishing and advertising, spam e-mails are also the perfect vehicle for the "pump-and-dump" scams that use false claims to promote penny stocks, driving up their prices so that a spammer can sell off his shares and bag a large profit. In September and November of last year, a group of six stock spammers was convicted of sending billions of spam e-mails to pump the share prices of 15 different public companies. Justin Medlin, extradited from Paris, was given the longest sentence: six years in a federal prison.

Denial of Service Attacks

Spammers typically use "botnets," herds of thousands of computers infected with malicious software, to send out millions of junk e-mails. But those zombie computers can also be put to a more malicious use. In 2004, Jason Michael Downey of Dry Ridge, Ky., used a botnet to attack competitors of his Internet Relay Chat network. Flooding his competitors' networks with fraudulent requests for data, he caused tens of thousands of dollars in damage to three other IRC networks. Last October, he was convicted for unlawful computer intrusion and sentenced to a year in federal prison.

Insider Sabotage

In October of 2003, Yung-Hsun Lin planted a piece of malicious software, a so-called "logic bomb," on the servers of his employer, Medco Health Solutions. Lin intended for software to "detonate" on his next birthday, April 23, 2004, erasing key files from the company's databases and--he hoped--giving him greater security as a systems administrator charged with fixing information technology problems. Instead, the logic bomb malfunctioned and was discovered by another employee in 2005. Lin was convicted of transmitting computer code with the intent to cause damage and sentenced in January to two years and six months in federal prison.

Insider Data Theft

Last May, David Haltinner of Menasha, Wisc., sold a database of 637,000 credit card numbers to two different customers in an online marketplace for stolen identities. Unfortunately for him, both of those customers turned out to be the one Secret Service agent. Haltinner was arrested and admitted to gaining access to the credit card numbers as, of all things, an information security analyst for a Wisconsin-based call center company. He was sentenced to four years and two months in federal prison in February.

Peer-To-Peer Identity Theft

On peer-to-peer file-sharing networks like Bittorrent or Limewire, users typically share music and videos. In 2006, Gregory Kopiloff found that many were accidentally sharing far more. Combing Limewire's network, he found that users were unknowingly giving the network's users access to their tax returns, student financial aid applications and credit card reports. Kopiloff used credit card and other stolen personal data to buy merchandise from the Web then resell it for cash. In mid-March, Kopiloff was sentenced to four years and three months in prison for mail fraud, accessing a computer without authorization to further fraud and aggravated identity theft.

Spying and Intimidation

If using the Internet to distribute child pornography wasn't disturbing enough, Ivory Dickerson of Orlando, Fla., took the dark side of the Web a step further. For several years, he hacked into minors' unsecured Web cams with the intention of filming them in secret and used Trojan software embedded in e-mails to take control of several minors' computers. Once Dickerson gained access, he sent instant messages to intimidate and threaten his victims, coercing them to film themselves engaged in pornographic acts. Last September, he received a life sentence in prison after pleading guilty to unlawful computer intrusion and possessing and manufacturing child pornography.

Exercício 6: Faça o que se pede a seguir:

A. Choose the best words to go into each of the spaces.

1. A person who illegally accesses somebody else's computer over the internet is called a _____.
   a. pirate **b.** hack **c.** hacker

2. A website which (in theory) cannot be accessed by a hacker is _____.
   a. strong **b.** secure **c.** clean

3. A website which can only be viewed by authorised people has _____ access.
   a. reduced **b.** small **c.** restricted

4. Unwanted advertising emails are popularly known as _____.
   a. meatloaf **b.** spam **c.** sausages

5. Software which blocks attempts by others to access your computer over the internet is called a _____.
   a. firewall **b.** fire blanket **c.** fire engine

6. It's essential to _____ your anti-virus protection regularly.
   a. up-to-date **b.** date **c.** update

7. Anti-virus software can _____ your computer for viruses.
   a. detect **b.** review **c.** scan

8. Anti-virus software can also _____ viruses on removable media, such as floppy disks.
   a. detect **b.** control **c.** see

9. When your anti-virus software subscription _____…
   a. ends **b.** stops **c.** expires

10. … it's a good idea to _____ it immediately.
    a. renew **b.** renovate **c.** replace

B. Match the malware with the damage. (It's not easy, and the terms are sometimes confused with each other.)

1. **virus**	a. collects and sends private information from the infected computer to a third party
2. **spyware**	b. an undesirable program which can replicate itself across a network
3. **trojan horse**	c. allows a hacker to access private information when he/she wishes
4. **keystroke logger** or **keylogger**	d. a program which adds itself to an executable file, and can cause considerable damage to the data on the infected computer
5. **worm**	e. records characters that are typed into a computer