

Discovering Computers 2016

Tools, Apps, Devices, and the Impact of Technology

Chapter 5

Digital Security, Ethics, and Privacy



Objectives Overview

Definisikan istilah, risiko keamanan digital, dan menjelaskan secara singkat jenis-jenis kejahatan dunia maya

Jelaskan berbagai jenis serangan Internet dan jaringan, dan jelaskan cara melindungi dari serangan ini

Diskusikan teknik untuk mencegah akses dan penggunaan komputer yang tidak sah

Jelaskan cara produsen perangkat lunak melindungi dari pembajakan perangkat lunak

Diskusikan cara kerja enkripsi, tanda tangan digital, dan sertifikat digital

Objectives Overview

Identifikasi perlindungan terhadap pencurian perangkat keras, vandalisme, dan kegagalan sistem

Jelaskan opsi yang tersedia untuk backup

Identifikasi risiko dan perlindungan yang terkait dengan komunikasi nirkabel

Mengenali masalah yang terkait dengan akurasi informasi, hak kekayaan intelektual, kode etik, dan green computing

Diskusikan masalah seputar privasi informasi

Resiko Keamanan Digital

- **Digital security risk** adalah setiap peristiwa atau tindakan yang dapat menyebabkan hilangnya atau rusaknya perangkat keras komputer atau perangkat seluler, perangkat lunak, data, informasi, atau kemampuan pemrosesan
- Setiap tindakan ilegal yang melibatkan penggunaan komputer atau perangkat terkait umumnya disebut sebagai **computer crime**
- **Cybercrime** adalah tindakan ilegal online atau berbasis Internet

Resiko Keamanan Digital



Resiko Keamanan Digital

Hacker

Cracker

Script kiddie

Corporate spies

Unethical
employees

Cyberextortionist

Cyberterrorist

Serangan Internet dan Jaringan

- Informasi yang dikirimkan melalui jaringan memiliki tingkat risiko keamanan yang lebih tinggi daripada informasi yang disimpan di tempat organisasi
- **Malware**, kependekan dari perangkat lunak berbahaya, terdiri dari program yang bertindak tanpa sepengetahuan pengguna dan dengan sengaja mengubah operasi komputer dan perangkat seluler

Table 5-1 Common Types of Malware

Type	Description
<i>Virus</i>	A potentially damaging program that affects, or infects, a computer or mobile device negatively by altering the way the computer or device works without the user's knowledge or permission.
<i>Worm</i>	A program that copies itself repeatedly, for example in memory or on a network, using up resources and possibly shutting down the computer, device, or network.
<i>Trojan horse</i>	A program that hides within or looks like a legitimate program. Unlike a virus or worm, a trojan horse does not replicate itself to other computers or devices.
<i>Rootkit</i>	A program that hides in a computer or mobile device and allows someone from a remote location to take full control of the computer or device.
<i>Spyware</i>	A program placed on a computer or mobile device without the user's knowledge that secretly collects information about the user and then communicates the information it collects to some outside source while the user is online.
<i>Adware</i>	A program that displays an online advertisement in a banner, pop-up window, or pop-under window on webpages, email messages, or other Internet services.

Serangan Internet dan Jaringan

How a Virus Can Spread via an Email Message

Step 1

Unscrupulous programmers create a virus program that deletes all files. They hide the virus in a word processing document and attach the document to an email message.

Unscrupulous Programmers



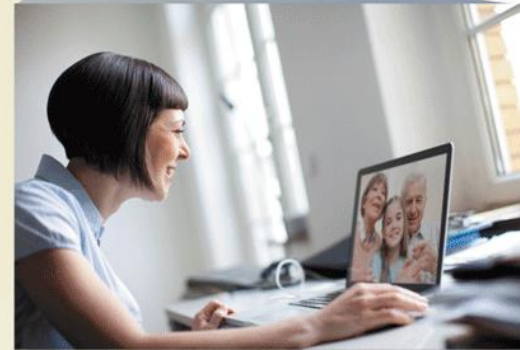
Step 2

They send the email message that contains the infected attachment to thousands of users around the world.



Step 3a

Some users open the attachment and their computers become infected with the virus.



Step 3b

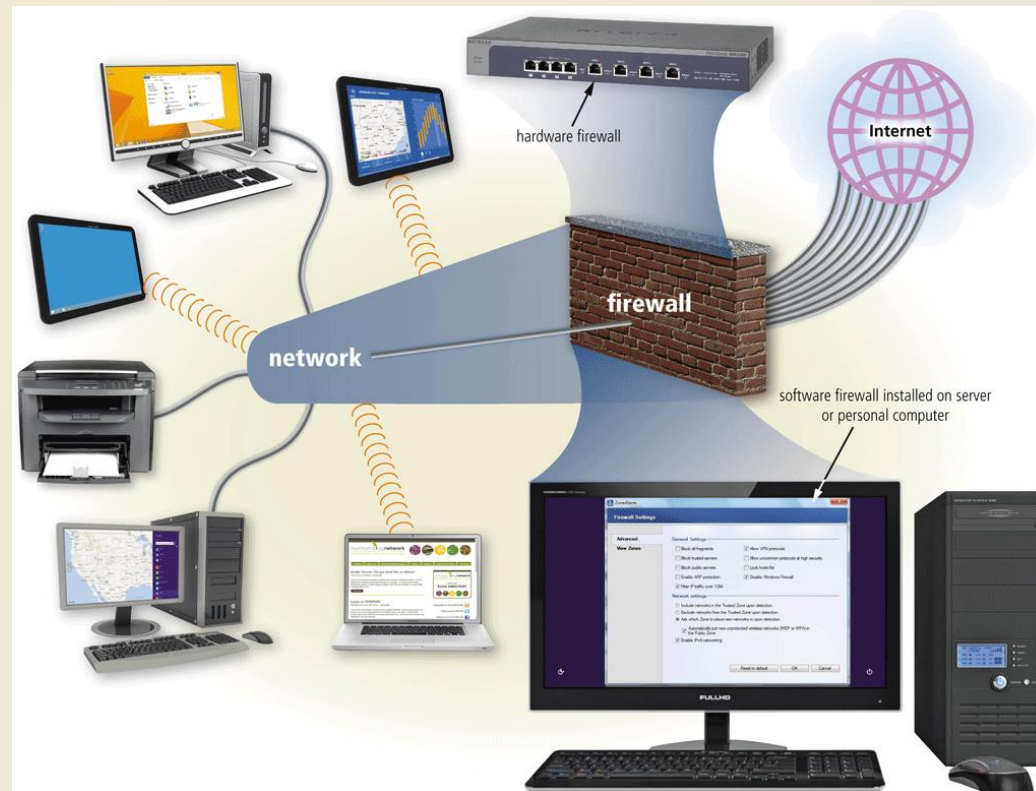
Other users do not recognize the name of the sender of the email message. These users do not open the email message — instead they immediately delete the email message and continue using their computers. These users' computers are not infected with the virus.

Serangan Internet dan Jaringan

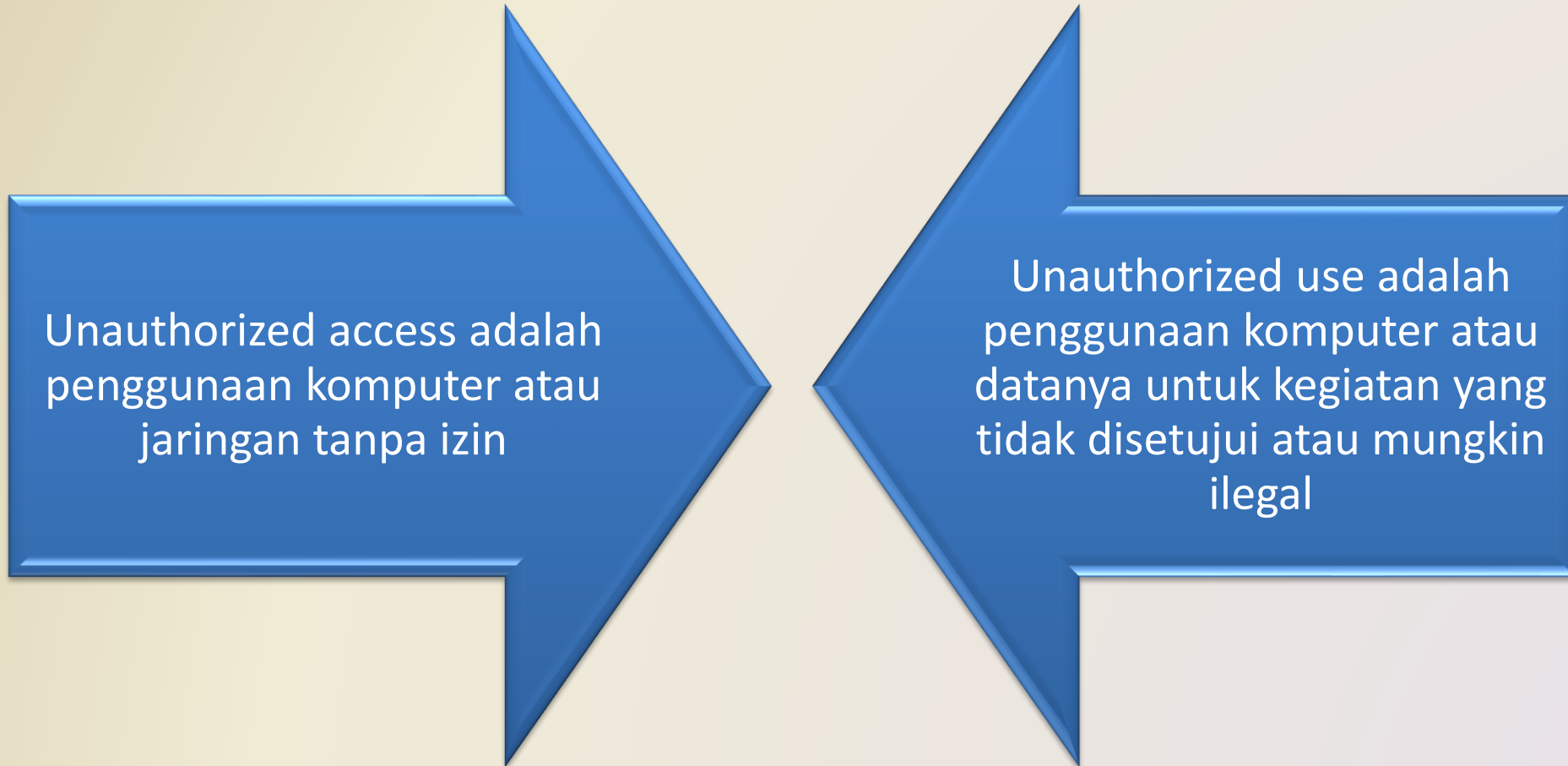
- **Botnet** adalah sekelompok komputer atau perangkat seluler yang disusupi yang terhubung ke jaringan
 - Komputer atau perangkat yang disusupi dikenal sebagai **zombie**
- **Denial of service attack (DoS attack)** mengganggu akses komputer ke layanan Internet
 - Distributed DoS attack (DDoS attack)
- **Back door** adalah program atau serangkaian instruksi dalam program yang memungkinkan pengguna untuk melewati kontrol keamanan
- **Spoofing** adalah teknik yang digunakan penyusup untuk membuat jaringan atau transmisi Internet mereka tampak sah

Serangan Internet dan Jaringan

- **Firewall** adalah perangkat keras dan/atau perangkat lunak yang melindungi sumber daya jaringan dari gangguan

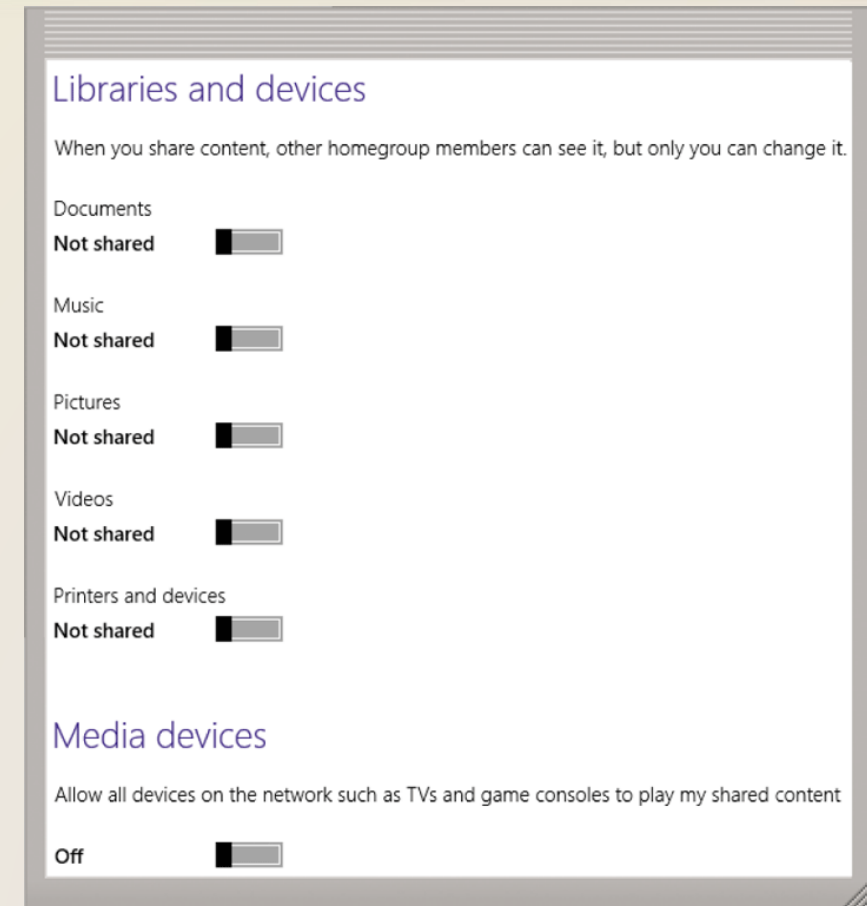


Akses dan Penggunaan Tidak Sah



Akses dan Penggunaan Tidak Sah

- Organisasi mengambil beberapa langkah untuk membantu mencegah akses dan penggunaan yang tidak sah
 - Kebijakan penggunaan yang dapat diterima
 - Nonaktifkan berbagi file dan printer



Akses dan Penggunaan Tidak Sah

- Kontrol akses menentukan siapa yang dapat mengakses komputer, perangkat, atau jaringan; kapan mereka dapat mengaksesnya; dan tindakan apa yang dapat mereka lakukan saat mengaksesnya
- Komputer, perangkat, atau jaringan harus memelihara jejak audit yang mencatat dalam file baik upaya akses yang berhasil maupun yang gagal

- **User name**
- **Password**



Akses dan Penggunaan Tidak Sah

- Frasa sandi adalah kombinasi kata pribadi, sering kali mengandung campuran huruf besar dan tanda baca, terkait dengan nama pengguna yang memungkinkan akses ke sumber daya komputer tertentu
- PIN (nomor identifikasi pribadi), kadang-kadang disebut kode sandi, adalah kata sandi numerik, baik yang diberikan oleh perusahaan atau dipilih oleh pengguna
- Objek yang dimiliki adalah barang apa pun yang harus Anda miliki, atau bawa bersama Anda, untuk mendapatkan akses ke komputer atau fasilitas komputer
- **Biometric device** mengotentikasi identitas seseorang dengan menerjemahkan karakteristik pribadi ke dalam kode digital yang dibandingkan dengan kode digital di komputer atau perangkat seluler yang memverifikasi karakteristik fisik atau perilaku

Akses dan Penggunaan Tidak Sah

**Fingerprint
reader**

**Face
recognition
system**



**Hand
geometry
system**

**Voice
verification
system**



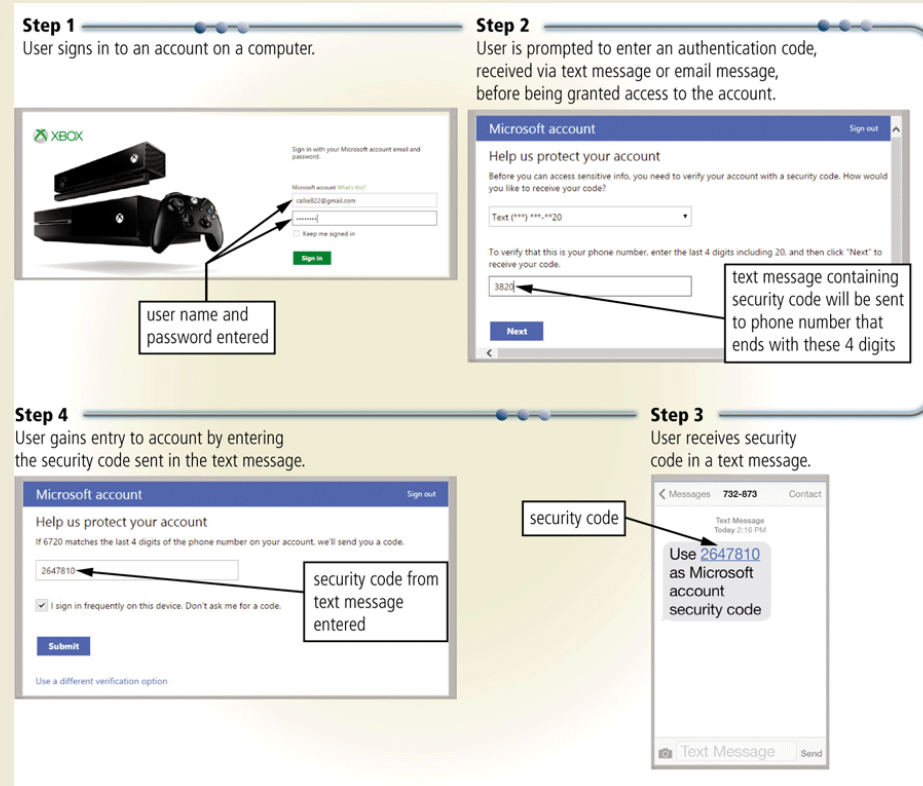
**Signature
verification
system**

**Iris
recognition
system**



Akses dan Penggunaan Tidak Sah

- **Dua tahapan verifikasi** menggunakan dua metode terpisah, satu demi satu, untuk memverifikasi identitas pengguna



Akses dan Penggunaan Tidak Sah

- **Digital forensics** adalah penemuan, pengumpulan, dan analisis bukti yang ditemukan di komputer dan jaringan
 - Banyak daerah menggunakan forensik digital



Software Theft

- **Software theft** terjadi ketika seseorang:

Mencuri media
perangkat lunak

Dengan sengaja
menghapus program

Secara ilegal
mendaftarkan
dan/atau
mengaktifkan program

Menyalin program
secara ilegal

Software Theft

- Banyak produsen memasukkan proses aktivasi ke dalam program mereka untuk memastikan perangkat lunak tidak diinstal pada lebih banyak komputer daripada yang dilisensikan secara legal
- Selama **aktivasi produk**, yang dilakukan baik secara online atau melalui telepon, pengguna memberikan nomor identifikasi produk perangkat lunak untuk mengaitkan perangkat lunak dengan komputer atau perangkat seluler tempat perangkat lunak diinstal.

Software Theft

- **License agreement** adalah hak untuk menggunakan perangkat lunak

Typical Conditions of a Single-User License Agreement

You can...

- Install the software on only one computer or device. (Some license agreements allow users to install the software on a specified number of computers and/or mobile devices.)
- Make one copy of the software as a backup.
- Give or sell the software to another individual, but only if the software is removed from the user's computer first.

You cannot...

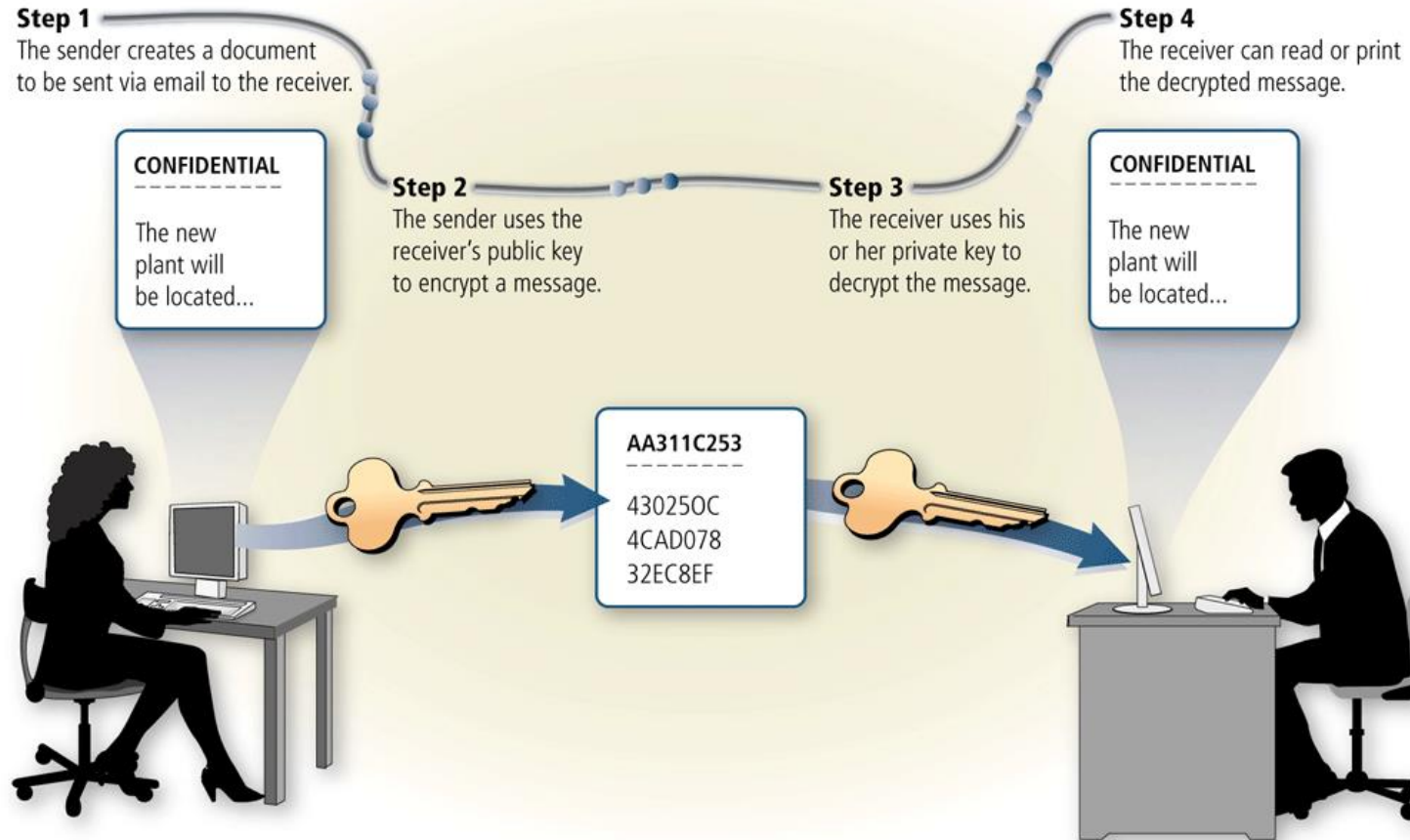
- Install the software on a network, such as a school computer lab.
- Give copies to friends and colleagues, while continuing to use the software.
- Export the software.
- Rent or lease the software.

Information Theft

- **Information theft** terjadi ketika seseorang mencuri informasi pribadi atau rahasia
- **Enkripsi** adalah proses mengubah data yang dapat dibaca oleh manusia menjadi karakter yang dikodekan untuk mencegah akses yang tidak sah

Information Theft

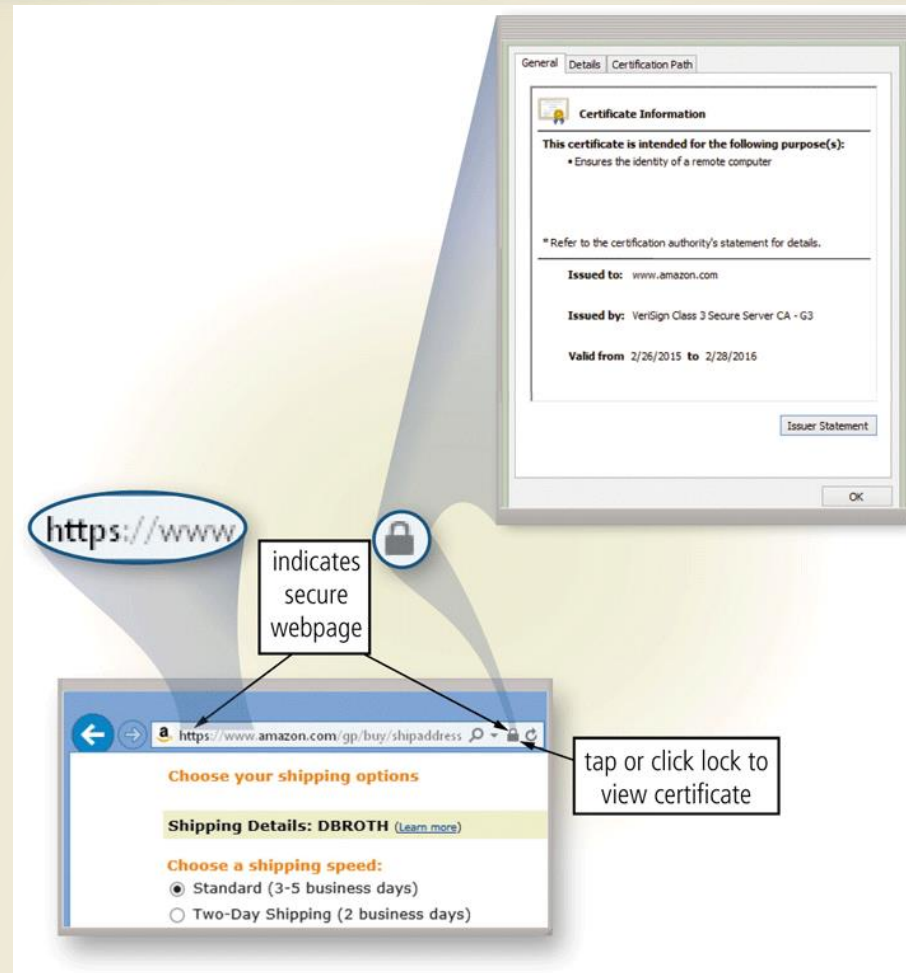
An Example of Public Key Encryption



Information Theft

- **Digital signature** adalah kode terenkripsi yang dilampirkan seseorang, situs web, atau organisasi ke pesan elektronik untuk memverifikasi identitas pengirim pesan
 - Sering digunakan untuk memastikan bahwa penipu tidak berpartisipasi dalam transaksi Internet
- **Digital certificate** adalah pemberitahuan yang menjamin keabsahan pengguna atau situs web
- Situs web yang menggunakan teknik enkripsi untuk mengamankan datanya dikenal sebagai **situs yang aman**

Information Theft



Pencurian Perangkat Keras, Vandalisme, dan Kegagalan

Pencurian hardware
adalah tindakan
mencuri peralatan
digital

Vandalisme perangkat
keras adalah tindakan
merusak atau merusak
peralatan digital

Hardware Theft, Vandalism, and Failure

Hardware Theft and Vandalism Safeguards

- Physical access controls (i.e., locked doors and windows)
- Alarm system
- Physical security devices (i.e., cables and locks)
- Device-tracking app

Hardware Failure Safeguards

- Surge protector
- Uninterruptible power supply (UPS)
- Duplicate components or duplicate computers
- Fault-tolerant computer



Backing Up

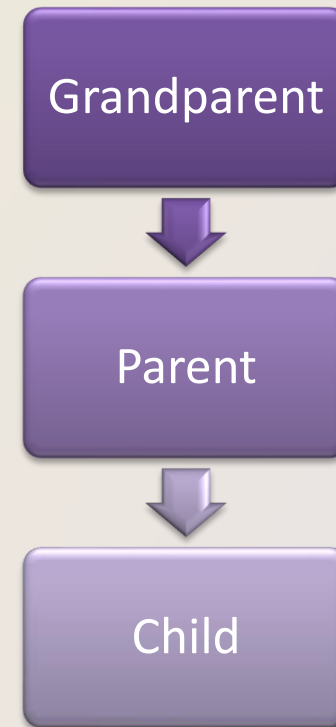
- **Backup** adalah duplikat dari file, program, atau media yang dapat digunakan jika yang asli hilang, rusak, atau musnah
 - Mencadangkan file berarti membuat salinannya
- Cadangan di luar situs disimpan di lokasi yang terpisah dari komputer atau situs perangkat seluler



Backing Up

- Kategori backups:
 - Full
 - Differensial
 - Tambahan
 - Selektif
 - Perlindungan data berkelanjutan
 - Cloud

- Kebijakan pencadangan tiga generasi



Backing Up

Table 5-2 Various Backup Methods

Type of Backup	Description	Advantages	Disadvantages
<i>Full backup</i>	Copies all of the files on media in the computer.	Fastest recovery method. All files are saved.	Longest backup time.
<i>Differential backup</i>	Copies only the files that have changed since the last full backup.	Fast backup method. Requires minimal storage space to back up.	Recovery is time-consuming because the last full backup plus the differential backup are needed.
<i>Incremental backup</i>	Copies only the files that have changed since the last full or incremental backup.	Fastest backup method. Requires minimal storage space to back up. Only most recent changes saved.	Recovery is most time-consuming because the last full backup and all incremental backups since the last full backup are needed.
<i>Selective backup</i>	Users choose which folders and files to include in a backup.	Fast backup method. Provides great flexibility.	Difficult to manage individual file backups. Least manageable of all the backup methods.
<i>Continuous data protection (CDP)</i>	All data is backed up whenever a change is made.	The only real-time backup. Very fast recovery of data.	Very expensive and requires a great amount of storage.
<i>Cloud backup</i>	Files are backed up to the cloud as they change.	Cloud backup provider maintains backup hardware. Files may be retrieved from anywhere with an Internet connection on any device.	Requires an Internet connection, otherwise files are marked for backup when the computer goes back online.

Wireless Security

- Wireless akses menimbulkan risiko keamanan tambahan
- Beberapa pelaku terhubung ke jaringan nirkabel orang lain untuk mendapatkan akses Internet gratis atau data rahasia
- Lainnya terhubung ke jaringan melalui titik akses nirkabel (WAP) atau kombinasi router/WAP



Etika Penggunaan Teknologi di Masyarakat

- **Technology ethics** adalah pedoman moral yang mengatur penggunaan komputer, perangkat seluler, sistem informasi, dan teknologi terkait
- Akurasi informasi menjadi perhatian
 - Tidak semua informasi di Internet itu benar



Etika Penggunaan Teknologi di Masyarakat

- Kekayaan intelektual mengacu pada karya unik dan orisinal seperti ide, penemuan, seni, tulisan, proses, nama perusahaan dan produk, serta logo.
- Hak kekayaan intelektual adalah hak yang menjadi hak pencipta atas karyanya
- Hak cipta melindungi segala bentuk ekspresi yang nyata
- Manajemen Hak Digital adalah strategi yang dirancang untuk mencegah distribusi ilegal film, musik, dan konten digital lainnya

Etika Penggunaan Teknologi di Masyarakat

- A **code of conduct** is a written guideline that helps determine whether a specification is ethical/unethical or allowed/not allowed

Sample IT Code of Conduct

1. Technology may not be used to harm other people.
2. Employees may not meddle in others' files.
3. Employees may use technology only for purposes in which they have been authorized.
4. Technology may not be used to steal.
5. Technology may not be used to bear false witness.
6. Employees may not copy or use software illegally.
7. Employees may not use others' technology resources without authorization.
8. Employees may not use others' intellectual property as their own.
9. Employees shall consider the social impact of programs and systems they design.
10. Employees always should use technology in a way that demonstrates consideration and respect for fellow humans.

Etika Penggunaan Teknologi di Masyarakat

- **Green computing** melibatkan pengurangan limbah listrik dan lingkungan saat menggunakan komputer, perangkat seluler, dan teknologi terkait

Green Computing Tips

1. Conserve Energy

- a. Use computers and devices that comply with the ENERGY STAR program.
- b. Do not leave a computer or device running overnight.
- c. Turn off the monitor, printer, and other devices when not in use.



2. Reduce Environmental Waste

- a. Use paperless methods to communicate.
- b. Recycle paper and buy recycled paper.
- c. Recycle toner and ink cartridges, computers, mobile devices, printers, and other devices.
- d. Telecommute.
- e. Use videoconferencing and VoIP for meetings.



Privasi Informasi

- **Information privacy** mengacu pada hak individu dan perusahaan untuk menolak atau membatasi pengumpulan, penggunaan, dan penyebaran informasi tentang mereka
- Basis data besar menyimpan data secara online
- Situs web sering mengumpulkan data tentang Anda, sehingga mereka dapat menyesuaikan iklan dan mengirimkan Anda pesan email yang dipersonalisasi
- Beberapa perusahaan memantau penggunaan komputer dan pesan email Anda

Privasi Informasi

How to Safeguard Personal Information



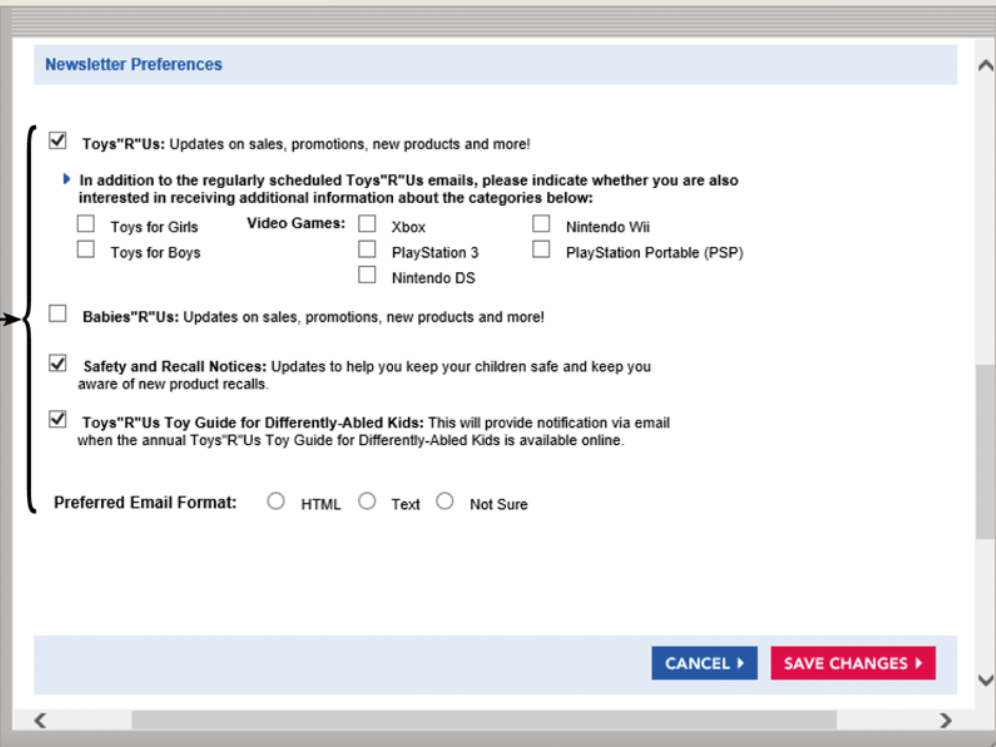
1. Fill in only necessary information on rebate, warranty, and registration forms.
2. Do not preprint your phone number or Social Security number on personal checks.
3. Have an unlisted or unpublished phone number.
4. If you have Caller ID, find out how to block your number from displaying on the receiver's system.
5. Do not write your phone number on charge or credit receipts.
6. Ask merchants not to write credit card numbers, phone numbers, Social Security numbers, and driver's license numbers on the back of your personal checks.
7. Purchase goods with cash, rather than credit or checks.
8. Avoid shopping club and buyer cards.
9. If merchants ask personal questions, find out why they want to know before releasing the information.

10. Inform merchants that you do not want them to distribute your personal information.
11. Request, in writing, to be removed from mailing lists.
12. Obtain your credit report once a year from each of the three major credit reporting agencies (Equifax, Experian, and TransUnion) and correct any errors.
13. Request a free copy of your medical records once a year from the Medical Information Bureau.
14. Limit the amount of information you provide to websites. Fill in only required information.
15. Install a cookie manager to filter cookies.
16. Clear your history file when you are finished browsing.
17. Set up a free email account. Use this email address for merchant forms.
18. Turn off file and printer sharing on your Internet connection.
19. Install a personal firewall.
20. Sign up for email filtering through your ISP or use an anti-spam program.
21. Do not reply to spam for any reason.
22. Surf the web anonymously or through an anonymous website.

Privasi Informasi

- Informasi tentang Anda dapat disimpan dalam database ketika Anda:
 - Isi formulir cetak atau online
 - Buat profil di jejaring sosial online
 - Daftarkan garansi produk

selecting these options means your preferences will be stored



The screenshot shows a 'Newsletter Preferences' form. It includes several checkboxes for selecting email updates: 'Toys"R"Us: Updates on sales, promotions, new products and more!' (checked), 'In addition to the regularly scheduled Toys"R"Us emails, please indicate whether you are also interested in receiving additional information about the categories below:' (with sub-options for Toys for Girls, Toys for Boys, Video Games, Xbox, PlayStation 3, Nintendo DS, Nintendo Wii, and PlayStation Portable (PSP)), 'Babies"R"Us: Updates on sales, promotions, new products and more!' (unchecked), 'Safety and Recall Notices: Updates to help you keep your children safe and keep you aware of new product recalls.' (checked), and 'Toys"R"Us Toy Guide for Differently-Abled Kids: This will provide notification via email when the annual Toys"R"Us Toy Guide for Differently-Abled Kids is available online.' (checked). At the bottom, there is a 'Preferred Email Format' section with radio buttons for HTML, Text, and Not Sure. The form has a blue 'CANCEL' button and a red 'SAVE CHANGES' button at the bottom right.

Privasi Informasi

- **Cookie** adalah file teks kecil yang disimpan oleh server web di komputer Anda
 - Situs web menggunakan cookie karena berbagai alasan:

Izinkan untuk
personalisasi

Simpan nama
pengguna
dan/atau kata
sandi

Bantu belanja
online

Lacak seberapa
sering pengguna
mengunjungi situs

Menargetkan iklan

Privasi Informasi

How Cookies Work

Step 1

When you enter the address of a website in a browser, the browser searches your hard drive for a cookie associated with the website.



Step 2

If the browser finds a cookie, it sends information in the cookie file to the website.

Step 3

If the website does not receive cookie information, and is expecting it, the website creates an identification number for you in its database and sends that number to your browser. The browser in turn creates a cookie file based on that number and stores the cookie file on your hard drive. The website now can update information in the cookie file whenever you access the website.

Privasi Informasi

- **Phishing** adalah penipuan di mana pelaku mengirimkan pesan email resmi yang mencoba mendapatkan informasi pribadi dan/atau keuangan Anda
- Dengan clickjacking, objek yang dapat disadap atau diklik di situs web berisi program jahat

Privasi Informasi

- **Spyware** adalah program yang ditempatkan di komputer atau perangkat seluler tanpa sepengetahuan pengguna yang secara diam-diam mengumpulkan informasi tentang pengguna dan kemudian mengomunikasikan informasi yang dikumpulkannya ke beberapa sumber luar saat pengguna sedang online.
- **Adware** adalah program yang menampilkan iklan online di spanduk atau jendela pop-up di halaman web, pesan email, atau layanan Internet lainnya

Privasi Informasi

- **Social engineering** didefinisikan sebagai memperoleh akses tidak sah ke atau memperoleh informasi rahasia dengan mengambil keuntungan dari sifat manusia percaya dari beberapa korban dan kenaifan orang lain

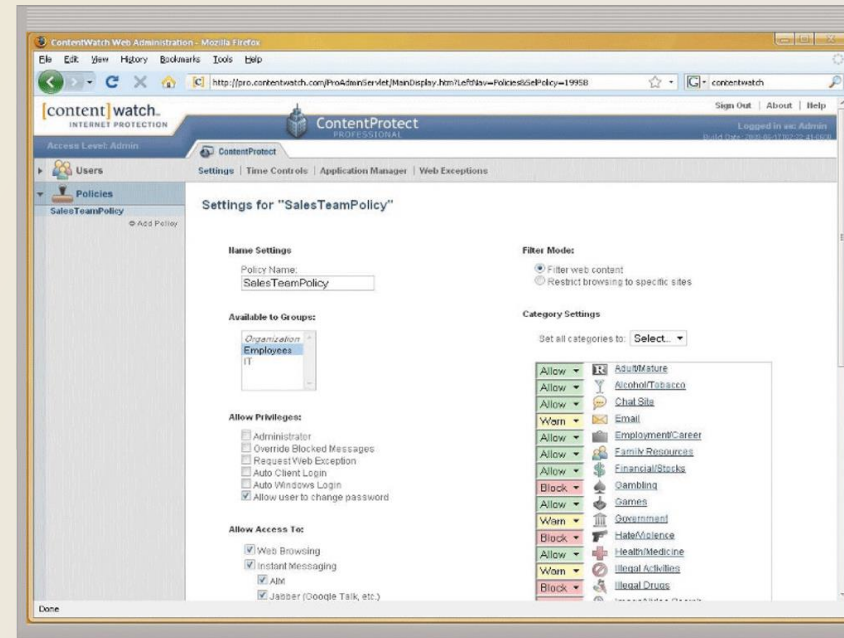
Privasi Informasi

Employee monitoring melibatkan penggunaan komputer, perangkat seluler, atau kamera untuk mengamati, merekam, dan meninjau penggunaan teknologi oleh karyawan, termasuk komunikasi seperti pesan email, aktivitas keyboard (digunakan untuk mengukur produktivitas), dan situs web yang dikunjungi

Banyak program ada yang dengan mudah memungkinkan pengusaha untuk memantau karyawan. Selanjutnya, adalah legal bagi pemberi kerja untuk menggunakan program ini

Privasi Informasi

- **Content filtering** adalah proses membatasi akses ke materi tertentu
 - Banyak bisnis menggunakan pemfilteran konten
- **Web filtering software** membatasi akses ke situs web tertentu



Discovering Computers 2016

Tools, Apps, Devices, and the Impact of Technology

Chapter 5

Digital Security, Ethics, and Privacy

Chapter 5 Complete

