

12.16: Security Issues in Information Technology

Learning Objectives

- Identify security issues associated with information technology.

Now that we have acknowledged the amount of data that business collects about people, what are the risks and challenges associated with keeping that information secure? Businesses stand to lose consumer confidence and respect if they allow unauthorized access to customer data. For this reason, businesses take information security and cyber-security seriously. Despite the importance of protecting customer data, breaches and hacks seem to be more and more common. Is this a result of inadequate security measures on the part of the businesses, or are hackers getting better at accessing so-called “secure networks”? The answer is probably both. In this section you’ll learn about some of the ongoing security issues businesses face in trying to safeguard their (and their customers’) electronic communications and data.

Information technology has presented businesses with opportunities undreamt of only a couple of decades ago. But it also has introduced some unprecedented challenges.



You can [view the transcript for “Home Depot Security Breach”](#) (opens in new window) or the [text alternative for “Home Depot Security Breach”](#) (opens in new window).

It has been estimated that businesses expend more than 5% of their annual IT budgets protecting themselves against disrupted operations and theft due to information theft. A February 2018 report by McAfee estimates that cyber-crime costs the world over \$800 billion or 0.08% of global GDP. Among the reasons given for the growing cost of cyber-crime are:

- Quick adoption of new technologies by cyber-criminals
- The increased number of new users online (these tend to be from low-income countries with weak cyber-security)
- The increased ease of committing cyber-crime, with the growth of Cyber-crime-as-a-Service
- An expanding number of cyber-crime “centers” that now include Brazil, India, North Korea, and Vietnam
- A growing financial sophistication among top-tier cyber criminals that, among other things, makes monetization easier

According to the McAfee report, “Monetization of stolen data, which has always been a problem for cyber-criminals, seems to have become

less difficult because of improvements in cyber-crime black markets and the use of digital currencies^[1].”

Cyber-crime can take on many faces from data breaches to malicious program that attack a company’s network and disrupt service or corrupt sensitive corporate data. We will examine just a few of the ways that criminals are using technology to wreak havoc on business operations.

Viruses and Malicious Programs

With the increased use of the Internet comes an increased risk of a business’s computer network being effected by malicious programs such as viruses. A computer virus is a piece of computer code that is inserted into another program and lies dormant until triggered by an unsuspecting user. This trigger can be as simple as opening a file attachment or downloading a file from the

Internet. Viruses range from the playful, simply displaying an image on the users' screen meant to be funny to extreme cases where data files are permanently erased. Most companies deploy anti-virus software across their network, but even the most sophisticated anti-virus software cannot keep up with the ever growing number of viruses and malicious programs out there. Motives for creating viruses can include seeking profit (e.g., with ransomware), desire to send a political message, personal amusement, to demonstrate that a vulnerability exists in software, for sabotage and denial of service, or simply because hackers wish to explore cyber-security issues. The consequences of such viruses and malicious programs can be catastrophic, effectively destroying a company's entire network and electronic records.

Phishing

One of the most prevalent cyber-attacks is the phishing scam. Phishing is when a scammer uses fraudulent emails or texts, or copycat websites to get you to share valuable personal information – such as account numbers, Social Security numbers, or your login IDs and passwords. Scammers use your information to steal your money or your identity or both. Scammers also use phishing emails to get access to your computer or network then they install programs like ransomware that can lock you out of important files on your computer.

Phishing scammers lure their targets into a false sense of security by spoofing the familiar, trusted logos of established, legitimate companies. Or they pretend to be a friend or family member. Phishing scammers make it seem like they need your information or someone else's, quickly – or something bad will happen. They might say your account will be frozen, you'll fail to get a tax refund, your boss will get mad, even that a family member will be hurt or you could be arrested. They tell lies to get to you to give them information.

To protect yourself and your company's information, the U.S. Federal Trade Commission recommends the following precautions:

- **Be cautious about opening attachments or clicking on links in emails.** Even your friend or family members' accounts could be hacked. Files and links can contain malware that can weaken your computer's security.
- **Do your own typing.** If a company or organization you know sends you a link or phone number, don't click. Use your favorite search engine to look up the website or phone number yourself. Even though a link or phone number in an email may look like the real deal, scammers can hide the true destination.
- **Make the call if you're not sure.** Do not respond to any emails that request personal or financial information. Phishers use pressure tactics and prey on fear. If you think a company, friend or family member really does need personal information from you, pick up the phone and call them yourself using the number on their website or in your address book, not the one in the email.
- **Turn on two-factor authentication.** For accounts that support it, two-factor authentication requires both your password and an additional piece of information to log in to your account. The second piece could be a code sent to your phone, or a random number generated by an app or a token. This protects your account even if your password is compromised.
- **Back up your files to an external hard drive or cloud storage.** Back up your files regularly to protect yourself against viruses or a ransomware attack.
- **Keep your security up to date.** Use security software you trust, and make sure you set it to update automatically.

Even with these precautions in place, highly sophisticated phishing scams are successful in achieving their goal. The following 2018 statistics from Dashlane (**SOURCE:** <https://blog.dashlane.com/phishing-statistics/>) illustrate just how prolific phishing attacks are:

- According to [PhishMe's Enterprise Phishing Resiliency and Defense Report](#), phishing attempts have grown 65% in the last year.
- According to Wombat Security State of the Phish, 76% of businesses reported being a victim of a phishing attack in the last year.
- According to the Verizon Data Breach Investigations Report, 30% of phishing messages get opened by targeted users and 12% of those users click on the malicious attachment or link.
- According to the [SANS Institute](#), 95% of all attacks on enterprise networks are the result of successful spear phishing.
- [According to Symantec, phishing rates have increased](#) across most industries and organization sizes — no company or vertical is immune.
- According to the Webroot Threat Report, nearly 1.5 million new phishing sites are created each month.

Another way that cyber-criminals interrupt business operations is through DoS (Denial of Service attacks).

Denial of Service

A denial-of-service (DoS) attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. Services affected may include email, websites, online accounts (e.g., banking), or other services that rely on the affected computer or network. A denial-of-service is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users. DoS attacks can cost an organization both time and money while their resources and services are inaccessible. In 2012, not one, not two, but a whopping six U.S. banks were targeted by a string of DoS attacks. The victims were no small-town banks either: They included Bank of America, JP Morgan Chase, U.S. Bancorp, Citigroup and PNC Bank.

These are just a few of the security issues associated with information technology. Such risks illustrate the need for increased cybersecurity to protect computer systems from theft or damage to their hardware, software or electronic data, as well as from disruption or misdirection of the services they provide. The field is of growing importance due to increasing reliance on computer systems, the Internet and wireless networks such as Bluetooth and Wi-Fi, and due to the growth of “smart” devices, including smartphones, televisions and the various devices that constitute the Internet of Things. Due to its complexity, both in terms of politics and technology, it is one of the major challenges of the contemporary world.

? Practice Question

<https://assessments.lumenlearning.co...essments/11103>

1. Lewis, James. "Economic Impact of Cybercrime—No Slowing Down." McAfee. January 2018. Accessed June 25, 2019. [csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf](https://prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf). ↵

Contributors and Attributions

CC licensed content, Original

- Security Issues in Information Technology. **Authored by:** Linda Williams. **Provided by:** Lumen Learning. **License:** [CC BY: Attribution](#)

CC licensed content, Shared previously

- Home Depot Security Breach. **Provided by:** BBC. **Located at:** <https://youtu.be/MHy8gKEmE48>. **License:** [CC BY-NC-ND: Attribution-NonCommercial-NoDerivatives](#)

12.16: Security Issues in Information Technology is shared under a [not declared](#) license and was authored, remixed, and/or curated by LibreTexts.

- 33.16: Security Issues in Information Technology has no license indicated.