

25.15: Electronic Communication

Learning Objectives

- Identify common risks associated with electronic communication
- Identify common ethical issues associated with electronic communication in business

Starting in the 1980s with the development of information and communications technologies, businesses have increasingly come to rely on electronic channels as a primary means of communicating and of conducting business. Such technological advances have been a tremendous boon, as businesses are now able to transmit and store vast amounts of information cheaply and quickly. At the same time, these developments are not without risks or challenges, particularly where ethics and security are concerned. In this section we discuss some of the concerns surrounding the use of electronic communication technologies.

Risks of Electronic Communication

Electronic communication and eCommerce have presented businesses with exciting opportunities that couldn't have existed even a couple decades ago. At the same time, they've brought unexpected challenges. Some of the biggest risks of using modern digital and electronic technology for communication and commerce are identity theft, unauthorized credit card or bank account use, and even demand for ransom for the return of stolen data.

When businesses allow customers to shop online, receive discounts by providing personal information, use live chat to communicate with customer service, they are hoping to enhance their image and provide a customer experience that is superior to the competition. But, what happens when the information a customer shares with a business is compromised or stolen by a third party? Consider what Home Depot endured when their customer database was breached in 2014:



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).



Data security is on everyone's mind these days, and the ways that electronic communication can be compromised seem to evolve as quickly as the technology. The following are just a few of the illicit and illegal ways that people get their hands on sensitive and private information:

- **Viruses, worms, and Trojan horses.** A computer virus is a type of malicious software program (“malware”) that, when executed, replicates by reproducing itself (copying its own source code) and/or infecting other computer programs by modifying them. A computer worm is a stand-alone malware computer program that replicates itself in order to spread to other computers. A Trojan horse, or Trojan, is any malicious computer program or phony site that is used to hack into computers by misleading users about its true intent or identity.
- **Spoofing or phishing.** Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons. Often the sender of the electronic communication is disguised as a trustworthy entity.
- **Denial-of-service attacks.** A denial-of-service attack (DoS attack) is a cyber attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting the services of a host connected to the Internet.

The low cost and rapid delivery of electronic communication makes it the preferred method of communication for both business and consumers, but there can be hidden hazards and costs. The following are common ones:

- **Electronic communications are forever.** Electronic messages are permanent (this includes communications such as email and also audio recordings such as voice mail). Even if a person deletes the communications from his or her own server or account, there are generally other servers that still hold this information. One way that these types of communications live in perpetuity is when they are sent or forwarded to multiple individuals.
- **Someone may be watching.** In many cases, confidential information is leaked by someone else sifting through his or her messages. The culprit may be a disgruntled employee or even a competitor. Workstations left unattended, employees remaining logged on to networks and email accounts when they are away from their desk, and even sharing passwords with coworkers all make it easy for prying eyes to see information not intended to be shared.
- **Innocent messages can still harm you.** Civil litigation lawyers will warn you that even innocent messages can get you in trouble if they are taken out of context. When a person writes an email or text, he or she may have only one intent or meaning in mind. However, messages can be misconstrued to apply to a completely different scenario.
- **Email avalanche.** Managers, in particular, are vulnerable to relying on email too heavily for communication. People use email because it’s quick and easy, and they can send the same information to a lot of people at the same time. This can lead to information overload and misunderstandings by recipients, however. Words alone account for only 7 percent of communication,^[1] so it’s important for managers to be aware of the limitations of email in getting their messages across.

? Practice Question

<https://assessments.lumenlearning.co...essments/14453>

Ethical Issues in Electronic Communication

Technology enables businesses to communicate and store information more readily and efficiently than ever. However, as much as technology impacts the way that companies do business, it also raises important new issues for the employer-employee relationship. If you send personal emails from your office computer, do you have the right to expect that they’re private? Does your employer have a legal and ethical right to “cyber-peek” at what you are doing with company assets? Twenty years ago this was not an issue; in 2010, it was a case before the Supreme Court. The case concerned the extent to which the right to privacy applies to electronic communications in a government workplace, and the city narrowly won. The U.S. Supreme Court has generally found in favor of employers, giving them the right to monitor any communication that occurs on their equipment (computers, smartphones, or pagers).



You can [view the transcript for “Cell Phone Privacy”](#) (opens in new window).

Employers want to use technology to help them screen applicants and verify information about their workforce, which is understandable. In the module on Human Resource Management you learned about the cost of recruiting, hiring, and training employees. However, what if the company believes that one of the quickest ways to gather information about an employee is to access their social media accounts? A company would never ask for your login credentials for Facebook, Twitter, Instagram, LinkedIn . . . or would they? And if they did, is it legally and ethically justified? What would you do if you found yourself in the situation presented in the following video?



You can [view the transcript for “US Employers Banned From Asking for Social Media Logins”](#) (opens in new window).

The fact is that technology has put our information at the fingertips of businesses—there for the taking and, in some cases, the selling. Is it ethical for a business to collect data about a person and then sell that information to another business? Many organizations collect data for their own purposes, but they also realize that your data has value to others. As a result, selling data has become an income stream for many organizations. If you didn’t realize that your data was collected by Company A, it’s even less likely you knew that it was sold to Company B.



You can [view the transcript for “Selling You As Data”](#) (opens in new window) or the [text alternative for “Selling You As Data”](#) (opens in new window).

? Practice Question

<https://assessments.lumenlearning.co...essments/14454>

1. Mehrabian, Albert (1981). *Silent Messages: Implicit Communication of Emotions and Attitudes* (2nd ed.). Belmont, CA: Wadsworth. ↵

Contributors and Attributions

CC licensed content, Original

- Revision and adaptation. **Authored by:** Linda Williams and Lumen Learning. **License:** [CC BY-SA: Attribution-ShareAlike](#)
- Practice Questions. **Authored by:** Robert Danielson. **Provided by:** Lumen Learning. **License:** [CC BY: Attribution](#)

CC licensed content, Shared previously

- Selling You As Data. **Provided by:** BBC. **Located at:** <https://youtu.be/nOyvHHWHYSo>. **License:** [CC BY-NC-ND: Attribution-NonCommercial-NoDerivatives](#)
- U.S. Employers Banned from Asking for Social Media Logins. **Provided by:** BBC. **Located at:** <https://youtu.be/vsjHABfgaLc>. **License:** [CC BY-NC-ND: Attribution-NonCommercial-NoDerivatives](#)
- Cell Phone Privacy. **Provided by:** BBC. **Located at:** <https://youtu.be/LVTvbpo8oH0>. **License:** [CC BY-NC-ND: Attribution-NonCommercial-NoDerivatives](#)
- Phishing. **Provided by:** Wikipedia. **Located at:** <https://en.Wikipedia.org/wiki/Phishing>. **License:** [CC BY-SA: Attribution-ShareAlike](#)
- Trojan Horse. **Provided by:** Wikipedia. **Located at:** [https://en.Wikipedia.org/wiki/Trojan_horse_\(computing\)](https://en.Wikipedia.org/wiki/Trojan_horse_(computing)). **License:** [CC BY-SA: Attribution-ShareAlike](#)
- Computer Virus. **Provided by:** Wikipedia. **Located at:** https://en.Wikipedia.org/wiki/Computer_virus. **License:** [CC BY-SA: Attribution-ShareAlike](#)
- Denial-of-Service Attack. **Provided by:** Wikipedia. **Located at:** https://en.Wikipedia.org/wiki/Denial-of-service_attack. **License:** [CC BY-SA: Attribution-ShareAlike](#)
- trojan_horse-9526. **Authored by:** Abraxas3d. **Located at:** <https://www.flickr.com/photos/w5nyv/6153652987/>. **License:** [CC BY-NC: Attribution-NonCommercial](#)
- City of Ontario v. Quon. **Provided by:** Wikipedia. **Located at:** https://en.Wikipedia.org/wiki/City_of_Ontario_v._Quon. **License:** [CC BY-SA: Attribution-ShareAlike](#)

25.15: Electronic Communication is shared under a [not declared](#) license and was authored, remixed, and/or curated by LibreTexts.