|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |
|  |
| Secure Computing  Frontline Medical Research |
|  |
| Information Technology Department |



# Security Awareness

N

ow that you are working from home, like most employees at Frontline Medical Research, you are probably using your computers and smartphones more frequently than ever before. Your computer is vulnerable to access by unauthorized systems, even when you sign into the company network for work tasks. Mobile devices increasingly risk attacks by viruses, spyware, and other malware. In fact, nearly one-third of the world’s computers could be infected with malware today[[1]](#footnote-1).

Mobile devices are especially vulnerable. Because of their very mobility, they can be easily lost, stolen, and accessed.



Following are three major steps you can take to protect your devices—and your personal and professional data.

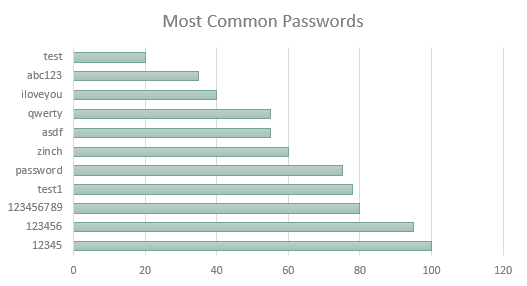
# Use Complex Passwords

Using secure passwords is the most reliable way to prevent illegal intrusions onto your devices and networks. The trick is to choose passwords that are easy to remember but difficult to guess. Passwords should contain at least eight characters—more than eight is preferable. It takes less than one second to crack a password that contains less than three characters. Following are tips for creating complex passwords:

1

* Use a long nonsense phrase. 
  + Include numbers, symbols, uppercase letters, and lowercase letters.
  + Avoid using personal information such as birth dates or street addresses.
* Use a different password for each website and account.
* Use a password manager to generate automatic passwords and keep track of them.
* Do not reuse passwords.

The top 20 passwords of all time include 123456, Password, abc123, and qwerty.



# Use Security Software

Install and use security software, and then keep it up to date. Security software includes a firewall, antivirus software, and antispyware. No device or operating system is safe from viruses or other types of malware.

2

## Installing and Activating Security Software

**firewall**: Operating systems have built-in firewalls, software designed to create a barrier between your data and the outside world. Before you go online with a new computer, make sure the firewall is turned on. Your broadband router also has a built-in hardware firewall.

**antivirus**: Computer viruses of all types infect your devices from email messages, websites, and vulnerabilities in your software and hardware. Viruses can slow your computer until it’s difficult to use, delete key files, or hold them for ransom.

**antispyware**: Spyware is software that secretly monitors your activities on a computer and collects personal or business data. You typically need software dedicated to finding spyware. You know you have it on your device if it displays unwanted ads or search results direct you to websites you didn’t select.

**updates:** Keep your operating system, apps, and browser up to date. They may seem like interruptions, but you should install all new updates because they include security fixes to prevent attackers from exploiting your data.

## Other Measures

Other ways to protect your devices and data are to ignore spam, back up your computer, and use two-factor authentication. Spam is unwanted email. Be suspicious of email messages from people and organizations you do not know. Phishing emails look legitimate but include links that provide information hackers can use to infiltrate your accounts. Frontline backs up business files on your hard drive laptop every night because the company has suffered the following types of cybersecurity attacks in the last five years.

Tips for using mobile devices include locking your device with a PIN or password. Never leave it unprotected in a public place. Install apps only from trusted stores and keep the operating system up to date.

|  |  |  |
| --- | --- | --- |
| Type | Description | Number of Attacks |
| DoS attacks | Network resources are jammed, preventing access. | 55 |
| Malicious scripts | Code runs at a low level to access data. | 84 |
| Ransomware | Malware encrypts files and demands payment. | 79 |
| Total | | 218 |

# Know the Numbers

Frontline Medical Research is not alone in combatting cybercrime. To give you a better idea of cybersecurity and its scope, the Information Technology Department collected statistics on security concerns for businesses and individual computer users worldwide. We reviewed information on data breaches and frequency and types of attacks.

3

| Type of Attack | Percentage (%) |
| --- | --- |
| Social engineering | 65 |
| Phishing and social engineering | 62 |
| Data breaches from hacking | 52 |
| Ransomware infections | 52 |
| Data breaches from malware | 28 |

As mentioned earlier, phishing is an email technique that attempts to trick users into providing confidential information. Social engineering is another type of deception. Another person or group of people attempt to manipulate you into divulging confidential or personal information and then use it for fraudulent purposes.

Data breaches are break-ins to a network without authorization. They often results in the theft of sensitive information, such as Social Security numbers. The number of widespread, well-publicized data breaches indicates that such breaches are becoming more common and frequent. They are also becoming more severe.

Do you want more information on cybersecurity? Send your requests to: [it@frontline.cengage.com](mailto:it@frontline.cengage.com)



Frontline Medical Research • IT Department •frontline.cengage.com

1. About 32 percent are infected, according to Tech World. [↑](#footnote-ref-1)