# IT Security Foundations: Core Concepts

with Lisa Bock

LEARNING

## Hyperlinks for each chapter

**Note: Links may change or be unavailable over time.**

## Chapter 1. Core Security Principles

### 01_01. Providing a secure system

- No links

### 01_02. Keeping information safe

- To view a live-attack map, visit: https://threatmap.fortiguard.com/

### 01_03. Managing risk

- No links

### 01_04. Analyzing risk

- No links

### 01_05. Avoiding scam artists

- Learn more about ways to avoid a social engineering attack by visiting: https://usa.kaspersky.com/resource-center/threats/how-to-avoid-social-engineering-attacks

### 01_06. Recognizing the Internet of Things

- Today, there are many devices that exist to improve our lives—learn more here: https://pioneerserviceinc.com/blog/the-industrial-internet-of-things-iiot-and-what-it-means-to-precision-machining/
- To see the extent of the possible attack surface of a single vehicle, go to: https://www.nccgroup.com/globalassets/newsroom/uk/blog/images/2017/07/car-attack-surface.png
- To reduce the threat of a cyberattack on your vehicle, secure your key fobs in bag that prevents someone from gaining access to the signal and disable in-car Wi-Fi—learn more here: https://www.mercuryinsurance.com/resources/auto/cyberattack-threats-to-your-vehicle-tips-for-protection.html
- Prior to purchasing an IoT device, do some research—learn more here: https://usa.kaspersky.com/resource-center/threats/secure-iot-devices-on-your-home-network
- Malicious actors can use a vehicle's key fob to gain access to your car; learn how this is done and ways to reduce the threat of an attack: https://lifehacker.com/how-to-keep-your-cars-key-fob-from-being-hacked-1847691268

# Chapter 2. Understanding Malware

## 02_01. Comparing malicious programs

- To view the effects of cyberattacks over the years, go to: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
- Malware has been around for quite a while, as outlined on this webpage: https://www.csoonline.com/article/3663051/11-infamous-malware-attacks-the-first-and-the-worst.html
- Read about Creeper and Reaper by going to: https://smartermsp.com/the-creeper-and-the-reaper-make-cybersecurity-history/
- For a visual on what you might see when Creeper was on the network, go to: https://upload.wikimedia.org/wikipedia/commons/e/eb/CreeperWorm.jpg
- For a discussion on the most common types of cyberattacks, visit: https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-cyberattacks/

## 02_02. Explaining viruses and worms

- Every day, over 450,000 variants of malware and potentially unwanted applications (PUAs) are registered by the AV-TEST Institute—learn more here: https://www.av-test.org/en/statistics/malware/

## 02_03. Eliminating unwanted surveillance

- Understand how spyware works, and ways to prevent this type of threat, by visiting: https://easydmarc.com/blog/what-is-spyware-and-how-to-protect-against-it/

## 02_04. Defending the OS

- Over time, advanced threats have become more aggressive and complex attacks, as shown in this graphic: https://static.seekingalpha.com/uploads/2022/3/14/49865266-16472947557780797.png
- Two sites that outline how **macOS** has multiple ways to defend against malicious activity:
  - https://support.apple.com/guide/security/protecting-against-malware-sec469d47bd8/web
  - https://www.security.org/antivirus/mac/
- If you are using a **Linux OS**, you have some choices on how you can defend against malware threats:
  - This site has a comprehensive list: https://linuxsecurity.expert/security-tools/linux-malware-detection-tools
  - Lynis is another malware scanning and vulnerability detecting tool that scans systems for security information and issues: https://cisofy.com/lynis/
- **Windows** has several tools that protect the OS:

- Microsoft includes Microsoft Defender Antivirus, which automatically activates if it does not sense that you have any antimalware protection: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-antivirus-windows?view=o365-worldwide
- If you feel your computer has become infected with malware, you could use the Microsoft Safety Scanner: https://docs.microsoft.com/en-us/microsoft-365/security/intelligence/safety-scanner-download?view=o365-worldwide
- More information on the Microsoft Safety Scanner, go to: https://answers.microsoft.com/en-us/windows/forum/all/microsoft-security-scanner-finds-infected-files/1fc86c29-4000-4e59-b940-292dad7ef058
- Data Execution Prevention (DEP) stops code from running in protected areas of a Windows OS—learn more here: https://docs.microsoft.com/en-us/windows/win32/memory/data-execution-prevention
- To verify the status of DEP settings in Windows 10, go to: http://www.thewindowsclub.com/verify-status-data-dep

### 02_05. Holding data hostage

- Ransomware attacks continue and affect all segments of public industry and private individuals—learn more here: https://www.comparitech.com/ransomware-attack-map/

## Chapter 3. Breaching Your System

### 03_01. Stopping the impostors

- To see a list of free online tools to look up potentially malicious websites, go to: https://zeltser.com/lookup-malicious-websites/
- If your computer becomes infected with malware, learn ways to remove it from your system: https://malwaretips.com/blogs/malware-removal-guide-for-windows/

### 03_02. Getting in the backdoor

- No links

### 03_03. Exploiting the unknown

- To view the many attacks that occur every day, go to Kaspersky Cyberthreat Real-Time Map: https://cybermap.kaspersky.com
- Understand how Microsoft defends against advanced threats by visiting: https://www.microsoft.com/en-us/microsoft-365/success/productivitylibrary/protect-detect-investigate-and-respond-to-advanced-threats

### 03_04. Challenge and response: Recognizing IoT threats

- The **Internet of Things (IoT)** poses unique challenges in managing information, as all systems are essentially interconnected.

- In the challenge, we'll go to this website: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/inside-the-smart-home-iot-device-threats-and-attack-scenarios
- List five possible ways IoT devices can be attacked

# Chapter 4. Investigating Internet Security

## 04_01. Accessing cloud resources

- Read *The Beginner's Guide to Understanding the Cloud and Cloud Computing*, found here: https://linchpinseo.com/guide-to-the-cloud/
- For a list of common software-as-a-service (SaaS) solutions, visit: https://joshfechter.com/software-service-examples/
- To view a graphic of the different types of cloud services in use today, visit: https://azurecomcdn.azureedge.net/cvt-f187b0e8321af2f3c7299619208c62b4c1e44f0eb595e2abd9bc3207f2c90b3e/images/page/resources/cloud-computing-dictionary/what-is-iaas/iaas-paas-saas.png

## 04_02. Using a secure connection

- Learn how you can tell if your connection is secure by visiting: https://support.mozilla.org/en-US/kb/how-do-i-tell-if-my-connection-is-secure

## 04_03. Accepting cookies

- Discover how Mozilla monitors sites for malicious cookie activity by visiting: https://support.mozilla.org/en-US/kb/enable-and-disable-cookies-website-preferences

## 04_04. Blocking malicious content

- To see an example of a web forgery attack, visit: https://conetix.com.au/wp-content/uploads/2014/01/28/ReportedWebForgeryError.png.pagespeed.ce.nTLCuHGCNB.png
- To learn how to turn off JavaScript, go to: https://www.privacypolicies.com/blog/enable-disable-javascript/#firefox
- To check if your browser is updated to the latest version, go to: https://updatemybrowser.org/

## 04_05. Ensuring browser privacy

- For an example of what you might see if you click on a malicious link, visit: https://www.itisatrap.org/firefox/its-an-attack.html
- Learn how all browsers compare by visiting: https://www.expressvpn.com/blog/best-browsers-for-privacy/
- This reference provides links on how to improve the privacy of most operating systems: https://www.techsafety.org/internetbrowserprivacytips
- When selecting a browser, you can compare privacy features here: https://privacytests.org/

# Chapter 5. Mobile and Wireless Security

## 05_01. Securing your home Wi-Fi

- To see the default password of a particular router, go to: https://www.routerpasswords.com/linksys-default-router-password/
- Once you get your router, change the default password to a secure password; here is an example: https://www.watchingthenet.com/wp-content/uploads/image/linksysnoadmin2.gif
- For a discussion on how to change your Wi-Fi password, go to: https://www.businessinsider.com/guides/tech/how-to-change-wifi-password
- To learn how to activate encryption on your router, visit: https://www.avast.com/c-how-to-turn-on-wifi-encryption-in-your-router-settings

## 05_02. Sharing a secret

- Learn more about the best encryption to use on your wireless network: https://www.howtogeek.com/782993/whats-the-best-wi-fi-encryption-to-use-in-2022/
- For recommended settings for Wi-Fi routers and access points, visit: https://support.apple.com/en-us/HT202068
- Test the strength of your password by visiting: https://www.security.org/how-secure-is-my-password/
- To view a sample of what you might see when setting up your router, visit: https://www.howtogeek.com/wp-content/uploads/2017/07/wpa_top.png.pagespeed.ce.hM4XhKhI0k.png

## 05_03. Concealing your access point

- No links

## 05_04. Protecting mobile devices

- To see a visual of how a man-in-the-middle (MiTM) attack works, visit: https://www.troyhunt.com/content/images/2016/02/30953094WiFi-Pineapple5.png
- Discover the Wi-Fi Pineapple by visiting: https://shop.hak5.org/products/wifi-pineapple

# Chapter 6. Secure Devices and Applications

## 06_01. Providing confidentiality

- To view what text looks like when encrypted, visit: https://codebeautify.org/encrypt-decrypt

## 06_02. Ensuring data integrity

- Learn more about hash functions by visiting: https://csrc.nist.gov/projects/hash-functions

- For a beginner's guide to hash functions, visit: https://www.thesslstore.com/blog/what-is-a-hash-function-in-cryptography-a-beginners-guide/
- Learn how a hash takes a variable-length input and produces a fixed-length output: https://sectigostore.com/blog/hash-function-in-cryptography-how-does-it-work/

### 06_03. Using cryptographic techniques

- Discover how cryptographic techniques can secure data, whether in motion or at rest: https://blogs.ucl.ac.uk/infosec/2017/03/12/applications-of-cryptography/
- Visit IBM's website and learn more about blockchain as a shared, immutable ledger for recording transactions: https://www.ibm.com/blockchain
- Learn how S/MIME secures email: https://learn.microsoft.com/en-us/exchange/security-and-compliance/smime-exo/smime-exo

### 06_04. Securing email

- Discover how spam is used in a phishing attack by visiting: https://www.dia.govt.nz/Spam-About-Scams-and-Phishing
- Email statistics in the US: https://www.statista.com/topics/4295/e-mail-usage-in-the-united-states/
- There are many websites available to send spoofed emails, visit one here: https://www.anonymailer.net/
- Be cautious before clicking a link in an email; however, if you are a victim of a phishing attack, report the attack here: https:/www.cisa.gov/uscert/report-phishing
- Take the phishing quiz to learn how to identify malicious email by visiting: https://phishingquiz.withgoogle.com

## Conclusion

### 07_01. Next steps

- To see a list of courses on my instructor page, visit: https://www.linkedin.com/learning/instructors/lisa-bock?u=104