Cybersecurity Fundamentals

Introduction

Getting started

10 Minutes

The internet is home to the biggest information sharing network ever created with billions of devices that communicate across the globe. In developed economies, the average person now owns multiple devices, which are essential to most aspects of daily life. In this digital landscape, everyone is susceptible to getting hacked. Cyber attacks impact large technology companies, financial institutions, media organizations, dating websites, political parties, small companies, and individuals just like us.

Cybersecurity is important because of the unprecedented amounts of data that we as individuals and organizations collect, store, and process on our electronic devices. As the volume and sophistication of cyber attacks grow, we are all tasked with safeguarding this information. Think about what we need to protect now and in our future!

- Individual and family privacy, finances, and health
- Business operations, trade secrets, and jobs
- Local and national government services
- Global commerce, safety, and even world peace

We must all take steps to protect our sensitive, personal information and business information.

> *The art of war teaches us to rely not on the likelihood of the enemy's not coming,*
> *but on our own readiness to receive him;*
> *not on the chance of his not attacking,*
> *but rather on the fact that we have made our position unassailable.*
>
> **— The Art of War by Sun Tzu (https://en.wikiquote.org/wiki/Sun_Tzu)**

Fast facts

Here are five fast, eye-opening cybersecurity facts to think about.

> The global average total cost of a data breach is **USD $4.24 million**, the highest it has ever been.
> **– Cost of a Data Breach Report 2021, IBM Security (https://www.ibm.com/downloads/cas/OJDVQGRY)**

> There will be a ransomware attack on businesses every **11 seconds** by 2021. This does not include attacks on individuals, which occurs even more frequently than businesses.
> **– Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021, Cybersecurity Ventures (https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/)**

> The average number of days it takes a business to fully recover from an attack is **287 days**.
> **– The State of Ransomware in the US: Report and Statistics 2020, Emsisoft (https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/)**

> Even after filtering, **1 in 3,000** email messages an organization receives will still contain malware.
> **– The State of Email Security in 2020, Fortinet (https://www.fortinet.com/blog/business-and-technology/state-of-email-security-more-spam-malware-phishing-ransomware-ahead)**

> Cybersecurity job opportunities will grow **33%** from 2020 to 2030, much faster than the average growth rate for all occupations.
> **– US Bureau of Labor Statistics (https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm)**

Welcome to this course

Welcome to this **Cybersecurity Fundamentals** course! This is an introductory learning experience. It is designed to provide you with an overview of cybersecurity to get you interested in understanding this dynamic and evolving field. The purpose of this course is to provide you with:

- Foundational knowledge about the field of cybersecurity
- An awareness of cybersecurity career opportunities that are in high demand globally

Course design and completion

Modules and lessons

You can easily navigate using the organized **module** structure at your own pace. This course has the following modules.

- **Overview of Cybersecurity**
  What is cybersecurity and its objectives? What are risk management methods, common misconceptions about cybersecurity, and laws to consider?
- **Cybersecurity: On the Offense**
  Who is attacking, how, and what are their motives?
- **Cybersecurity: On the Defense**
  How can organizations protect against, detect, and respond to attacks?
- **A Career in Cybersecurity**
  What is the job market like and what skills would you need if you are interested in starting a career in cybersecurity?

Each module has a series of **lessons**. In each lesson, you will find the course information, supporting graphics, self-reflection activities, and short research activities.

The course is designed for you to complete the modules and lessons in sequential order.

Completion

Some lessons conclude with a mini quiz to check your understanding of the content. You must pass these mini quizzes in order to get completion credit for the particular lesson. The scores are not tracked.

When you complete a lesson, check **I've checked it out!** at the bottom of the page to collect your credit and confirm completion!

Then, click **Let's Keep Going!** to continue to the next lesson in the course. You will see a check mark when you complete lessons and modules.

There is a final, graded quiz called **Show What You Know** at the end of the course. You must achieve **80 percent** to pass. Don't worry! If you aren't successful at first, you can retake the quiz as many times as needed to pass.

Duration

The course is estimated to be approximately **six hours**.

> **Tip!** This course is quite long in duration. It is highly recommended that you pace your learning over a period of time that works for you and your schedule. For instance, you can complete a lesson and then come back to pick up where you left off. Your progress is tracked.

Badge

You have the opportunity to earn the **Cybersecurity Fundamentals** badge once you complete all course components. Please allow a few business days for processing. You will receive an email to claim the badge online.

Course author

Robert Calvert
IBM, United Kingdom

Robert Calvert is a cybersecurity professional working at IBM within Cloud security. In addition to his role at IBM, he has been involved in shaping several training initiatives within the UK. Robert educates a diverse range of new professionals to the security industry from many walks of life. Successful programs include those tailored toward early professionals starting their first role and military veterans changing careers.

What is cyberspace?

Let's get you thinking by considering two contrasting definitions of the term **cyberspace**. Please read each definition.

Definition #1	**Definition #2**
The interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems, internet - connected devices and embedded processors and controllers. It may also refer to the virtual world or domain as an experienced phenomenon, or abstract concept.	A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data.
Source: **National Cyber Security Strategy 2016-2021 (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf)**, United Kingdom, GOV.UK, September 2017	Source: **Neuromancer (https://en.wikipedia.org/wiki/Neuromancer)**, by William Gibson, 1984

What do you think about the two definitions?

Let's evaluate. The first definition is a text book definition. The second definition is from a science fiction novel called Neuromancer by American-Canadian writer William Gibson. The novel was one of the sources of inspiration for The Matrix series of films and it provided inspiration for computer scientists in the 1990s.

The fact that cyberspace was defined over 35 years ago and has come to be truer than ever before is awe inspiring. The statistics concerning modern technology are outstanding. They are exactly what was predicted. Today, there are billions of users across the world, every device is connected, there is complexity beyond human understanding, and there is unimaginable beauty.

The digital world is much more than just a network of computer systems. It is a place where people do business, live, love, and ultimately are immortalized.

Cyberspace is the crazy world in which cybersecurity professionals work. They strive to protect the world from those who would do it harm. They remain vigilant, focused, and unwavering in perusing objectives.

The stakes have never been higher. Should they fail, our modern way of life is threatened from the values we hold dear to the infrastructure we rely on for every aspect of our lives. The nightmares we dream would become everyone’s new reality.

Hopefully considering these definitions of cyberspace made you reflect on your views about the internet and wish to engage in its future. This course can start you on your cybersecurity journey. Let's begin!