eDynamicLearning

CAREER & ELECTIVE COURSES

INFORMATION TECHNOLOGY

Cybersecurity 1a

Foundations

Course Syllabus

Cybersecurity 1a: Foundations

Course Code: EDL098

Course Description

We depend more and more on the technologies we interact with every day, and we put more and more of our personal data out there online. Can all of that data really be kept "secret"? We all need to know more about how to protect our personal information, especially given how much we rely on and use our network devices and media. You'll learn about the various parts of your computer, how they work together, and how you can manipulate them to keep your data safe. You'll also dive into the tools, technologies, and methods that will help protect you from an attack and discover the many opportunities in the rapidly growing field of cybersecurity.

Required Materials

- Slide-show presentation program
- Word processing program

Software:

Virtual Box: https://www.virtualbox.org/wiki/downloads

In order to run VirtualBox on your machine, you need:

- CPU: Recent Intel or AMD processor
- Memory: 2+GB RAM
- Hard disk: About 4GB free hard disk space
- Supported Operating System: Windows, Mac OS X, Linux, Solaris and OpenSolaris.

Other Materials

- USB memory stick (Recommended to be at least 4 GB)

Optional Materials

(The following materials will only be needed if student chooses to do some activities/labs by hand.)

- Printer
- Blank paper (a variety of sizes)
- Markers, crayons, pens, pencils

Note: Your state's standards for this Cybersecurity course may require students to purchase and to install security equipment. Check with your school's administration to determine if this is necessary for course completion. This course provides alternate activities that could address these standards.

Table of Contents

Unit 1: Basics of Cybersecurity

Unit Summary

Today, people carry the world around in their pockets. That's right—the world. At any given moment, we have the power to seek, find, and interact with just about any kind of information we want via the internet. But it's not all open doors and friendly faces out there in cyber space. As we continue to navigate our online landscape, it becomes clear it can be a dangerous place indeed, especially if we don't take the right precautions. Passwords, codes, verification questions—these all serve as watchdogs for our data, but it's important to remember there are also clever people out there who are adept at sneaking around these safety measures. By looking critically at the connectivity of the internet, it's easy to see how the pathways of communication can also become avenues for attack. This is the founding notion behind cybersecurity and the exact reason why—many years and several hundred billion dollars later—its efforts still struggle to keep pace with hackers and online threats. And in this brave new cyber reality, learning the ins and outs of the world you carry in your pocket has never been more important.

Learning Objectives

- Use cybersecurity terms effectively
- Explain the essential differences between cybersecurity and information assurance
- Describe the importance of information within cyberspace
- Understand the security triad model, or the AIC triad, and how it relates to cyber security

Unit 2: Computers and Operating Systems

Unit Summary

Our personal computers, tablets, and smartphones offer different user options, but they all have one thing in common—operating systems. Since an operating system (OS) is what makes everything on your device run smoothly, it would be pretty terrible if it were to be compromised. Recognizing how our OSes govern what our technology can do is an important part of being a savvy user and crucial to effective cybersecurity. Being a well-protected online adventurer demands more than just a basic understanding of the computer itself; it requires some knowledge about the strengths and weaknesses of the components that live inside the device as well.

Learning Objectives

- Compare and contrast memory technologies
- Identify different kinds of software and how they apply to cybersecurity
- Explain the differences between operating systems and how they compare
- Understand basic computer components, as well as their functions and operation

Unit 3: Networking Fundamentals

Unit Summary

When people “network,” they come together to share information and stay connected. And in that way, you can have a network of friends, a network of systems, or a network of ideas. Computers are similar —they must also join together for the purpose of sharing resources and communicating. This can include sharing anything from a printer to a file server, but the most valued and popular resource today for human connection is the internet. Once we begin to learn how a network really functions and what it can do, it will be easier to understand the vast and complicated world of cybersecurity. Sharing ideas, images, and resources is what makes the world go ‘round, and networks are what form the backbone of this new reality. As the ways and means of connecting and sharing become increasingly complex, so will our need to secure our computer networks, and developing them in innovative ways will become one of the most important challenges we face.

Learning Objectives

- Describe the different computer networks, their characteristics, and how they function
- Explain how the seven layers of the Open Systems Interconnection (OSI) model function
- Compare and contrast network topologies
- Identify the different protocols commonly used in a network environment

Unit 4: Network Security

Unit Summary

Some people might say we already have all the tools we will ever need to protect ourselves from cyberattacks; we just need to learn from the world around us and find ways to use them effectively. Humans have been in conflict since the beginning of time, and technology's new landscape of virtual warfare is simply an extension of this ongoing condition—the modern battlefield, if you will. Just as our weapons arsenal has expanded over thousands of years from clubs and arrows to machine guns and bombs, the practices of cybersecurity are in the midst of their own mighty evolution. Understanding how a network provides the backbone for communication is just one step in visualizing how we can protect the vitality of our online platforms. From application security to firewalls, guardianship of our virtual world is no small task. But if the defenses of the real world are any indication of our ability to protect ourselves, there's always a way to stay ahead of any threat. We just have to learn how.

Learning Objectives

- Describe how to configure and assess the security of firewalls
- Explain how network configuration factors into cybersecurity
- Identify key components of network security and how they can be achieved
- Understand how the performance, efficiency, and security of a network can be established and maintained

Midterm Exam

Learning Objectives

- Review information acquired and mastered from this course up to this point.
- Take a course exam based on material from the first four units in this course (Note: You will be able to open this exam only one time.)

Unit 5: Access Control

Unit Summary

One of the biggest vulnerabilities in technology today is the lack of access control. If an online attacker is able to find just the right code, password, or tactic to gain passage through certain obstacles, the treasure of personal data is ripe for the picking. In this way, access is the prized gateway and the main objective of any savvy cybercriminal. And as such, access control is also a security point that requires the utmost attention and support. Understanding how data can be accessed (and what can be done to prevent it) sits at the core of any meaningful cybersecurity effort. Doors of entry and the locks that protect them—in the real world and the cyber one—come in all shapes and sizes, and you need to understand every inch of this digital environment if you hope to protect it.

Learning Objectives

- Understand how to properly secure a computer network
- Explain various methods of access control in computer security
- Explore the benefits of using a virtual private network (VPN)
- Describe the basic methods of authentication and remote access control

Unit 6: Mobile Devices and Cloud Computing

Unit Summary

These days, everybody wants their internet connection wherever and whenever they feel like checking in with work and friends, or any other wide array of internet services. And luckily for them, the invention of mobile devices with full operating systems and network accessibility has made that desire a reality. In fact, experts say 70 percent of all online activity is now generated through some kind of mobile use, which means all the security measures originally designed for those big desktop computers must now be applied to our smartphones and other portable devices in a myriad of new ways. It turns out that virtual and wireless worlds, complete with cloud computing abilities that can store, process, and transit information on the go, offer a lot of technological convenience, but unfortunately, they have also introduced a great deal of cyber risk.

Learning Objectives

- Identify the possible exploits in mobile applications
- Understand and assess the security of mobile devices
- Demonstrate an understanding of virtualization technology
- Explain common risks associated with wireless networks

Unit 7: Protecting Data

Unit Summary

Although it can be tempting to place our most precious assets under lock and key, such a heavy-handed security approach is just not practical. Digitally speaking, your information must have the freedom to move around the internet—connecting, sharing, transmitting, and making the technological world turn. So, the question then becomes, "How do you keep data safe while still allowing it to roam freely?" The answer is two-fold, as it demands a thorough understanding of both the physical and virtual realms of cybersecurity. Now that you understand the paths data takes while traveling through networks and the hardware involved with keeping it safe, it's time to dig into encryption, application security, and other effective ways to "harden" and safeguard your valuable data. If walking along a well-protected road makes you feel more confident, you will likely appreciate how cybersecurity's layered approach is akin to camouflaging yourself or traveling in a bulletproof car. In the event of a real threat, even the smallest additional protections could be helpful. In reality, hackers are likely never going to disappear entirely, which means our approach to safety in our journey through cyberspace must be balanced, well-rounded, and as thorough as possible.

Learning Objectives

- Recognize what it means to protect data in motion
- Identify effective methods of data protection, both physical and virtual
- Understand the history of encryption and how it is used in a digital setting
- Evaluate environmental controls and other components of physical security
- Describe the different processes involved with secure data use and disposal
- Explain the techniques of system hardening and how they protect computer systems

Unit 8: Trends and Challenges

Unit Summary

Just like any profession, recognizing the current trends and challenges within the cybersecurity field is one of the best ways to truly understand it. From cyber terrorism to ransomware attacks to the Internet of Things, the digital landscape of today is far more complicated and dangerous than ever before. Establishing proper habits of digital citizenship and taking responsibility for your online information are just a couple of the ways you can become a well-seasoned and knowledgeable professional. The digital arms race between malicious actors and the powers of good has never been more heated, as individuals around the globe struggle to predict and understand the many ways an attack can harm vital infrastructure and threaten human life. This is no small effort and demands that experts and users alike stay vigilant, well-informed, and ready to fight for their digital safety.

Learning Objectives

- Define cyber terrorism and the way it threatens public infrastructures
- Explain the Internet of Things (IoT) and its significance in cybersecurity
- Recognize current trends in cyberattacks and the strategies used to combat them
- Identify the key legislative acts that impact cybersecurity
- Understand the larger process of pursuing cybersecurity as a professional skillset

Final Exam

Learning Objectives

- Review information acquired and mastered from this course up to this point.
- Take a course exam based on material from units five to eight in this course – the last four units. (Note: You will be able to open this exam only one time.)