Cyber Explore Course Transcript

Please note that transcripts for the five videos in this course are included within the transcript text. This course has no narration or voice-over.

You may be asking yourself…Do I really need to take this course? Yeah, you do.

Begin Video Script.
Hacker: Why should you take this course? Between you and me, I wish you wouldn't. If ignorance is bliss, I'd be happy as a clam if you were clueless as to the inner workings of your desktops, laptops, and devices because those, my friend, are my playground. You keep on believing that cyber phishing is a high-tech vacation activity, and I'll keep on e-mailing, that and a whole lot more, so do me a favor. Skip this course. Pretend I don't exist. Make my day, punk, and pretty soon, your data is mine. Toodles...for now.
End Video Script.

“The United States is the number one target for foreign-based cyber operations.” - Bill Evanina, Director of NCSC

Video: The National Counterintelligence Executive and Director of the National Counterintelligence and Security Center

Begin Video Script.
Mr. Bill Evanina, Director of NCSC: Hello, I'm Bill Evanina, the National Counterintelligence Executive and Director of the National Counterintelligence and Security Center or NCSC. Our mission is to lead an integrated national counterintelligence and security effort against foreign intelligence and insider threats to the United States and its interests worldwide.

We accomplish our mission using a "whole of nation" approach, necessitated by the reality that sensitive national security information is no longer held strictly by the Intelligence Community nor always classified. To identify and mitigate the risk of our nation's sensitive information, counterintelligence and security work together, examining the capabilities and intent of our adversaries and addressing the vulnerabilities those adversaries could exploit. These foreign intelligence entities actively recruit personnel with access to sensitive national security information. But insider threats don't just come from foreign intelligence entities.

NCSC continues to work with the Intelligence Community, other government departments and agencies, and private industry to develop policies, guidelines, and training that will assist in establishing insider threat detection and awareness programs. The United States is the number one target of foreign-based cyber operations. Our nation relies on its cyber infrastructure for everything from communications, to management of critical infrastructure, to command and control of our military. Our training programs are specifically designed to raise your awareness and, in turn, your ability to identify and counter sophisticated threats to our national security, both from foreign intelligence entities and malicious insiders.

I charge each of you to advance counterintelligence and security excellence every day. Thank you.
End Video Script.

Every network and device has vulnerabilities, some inherent, some self-imposed. Our foreign adversaries are forever seeking opportunities to infiltrate and exploit these vulnerabilities. Nearly seventy-five percent of all legitimate websites have unpatched vulnerabilities. Attackers reside within a network an average of eight months before they are even detected. Eighty-nine percent of all cyber attacks involve financial or espionage motivations.

Before you can fully understand the threat, you need to have a good foundation in the fundamental operations and capabilities of a computer and its networks. At the end of this course, you will understand how foreign adversaries could infiltrate and exploit our cyber networks through inherent and/or self-imposed vulnerabilities and the security procedures you can implement to help mitigate the risk.
Vulnerabilities lie within 3 areas: Technology, Configuration, and Security. During this course, you will EXPLORE these areas, giving you a foundation to help you progress through the Cyber Fundamentals series.

Modules and Objectives

Vulnerabilities
At the end of Module 01, you will be able to identify the computer's component layers and associated functions.

Attacks
At the end of Module 02, you will be able to recognize virtualization concepts.

Security Protection
At the end of Module 03, you will be able to choose the correct security protection associated with a computer's component layer.

Module 1 Cyber Basics

Unless you've been living off the grid, you use some form of technology. For many of us, we are conditioned to press the power button, then retreat into our own world, focused on the applications that apply to us.

"I work for the government…surely it has protocols in place to prevent hacking from occurring?" Many times it does, but hackers are ingenious; they can find ways in. There have been several governmental and corporate breaches, many were due to lack of encryption.

Why is it important for you to understand cyber technology? First, the very nature of your job revolves around some form of tracking, monitoring or securing intelligence against foreign adversaries much of this information is centered around cyber.

Second, the knowledge you learn in this course can be transferred and used in your personal life. YES. You need to understand how to protect your personal information, and limit your cyber footprint, decreasing your chances of becoming a target. This course will help.

Let's take a look at your computer. Understanding this is half the battle. A computer has three "layers."

1. Hardware: Motherboard, RAM, CPU
2. Operating System (O/S): MacOS, Linux, Windows
3. Applications: Excel, Google, Chrome

Much like a house, the foundation (Hardware) has to be built before installing the walls (O/S), then finally the roof (Applications). When you power on your computer from a complete shutdown, you might see a blue or black screen that quickly displays a lot of "stuff." This is your O/S (layer 2) starting. Let's talk about what is happening behind the scenes. You will see the following terms flash by: BIOS, Kernel, Ports, CPU. BIOS (basic input/output system), aka system set-up, is the program a computer's processor uses to get the system started when powered on. It instructs the computer on basic functions such as booting. It can also manage data flow between the computer's O/S and attached devices, such as a hard disk, keyboard, mouse, and printer. Your O/S allows you to "work" on your computer. Think of it as the "communication middleman" between the Hardware and the Applications. The O/S allows the two layers to "talk" with each other. The Kernel is the "Middleman" (AKA communication) component. It represents the central module of the Operating System (O/S). Though the term Port sounds like a physical plugin, it is not. It is a representative number (e.g., 25, 80,443, etc.), assigned to certain types of communication traffic (e.g., email, web browsers, etc.) which allows the computer (O/S) to know how to route the information. For example, most email traffic across the world is assigned Port 25; most web browser (http) traffic is assigned Port 80; and secure browsers (https) are assigned 443.

These ports allow the computer to identify what is email or web data. Now that your O/S knows the type of traffic, it can route it through the correct server. "Many times, I get confused between the terms CPU and server. HELP!" The confusion is understandable. Many people use the terms interchangeably; however, they are different. A CPU (aka the processor) is the brains of a computer. It is a piece of hardware (e.g., Intel chip) that sits on the motherboard, and handles all of the instructions you give your computer. A server is a computer program that provides services to (aka manages) other computer programs. Several users can connect to a server at the same time. It is challenging for the average user to see the distinction. Every computer has a CPU, but not every computer operates as a server.

Module 1 Knowledge Check
Use your knowledge of the three layers and their function to select the best answer. Then click the arrow for the next question.

What are the three layers of a computer?

a. Bottom, middle, top
b. Hardware, operating system, applications
c. CPU, operating system, applications

d. None of the above

The correct answer is b.
The computer has three layers, hardware, operating system, and applications.

Which of the following would be found in the hardware layer?

a. Google Chrome, Internet Explorer, Microsoft Office
b. Linux, Windows, or macOS
c. CPU, motherboard, RAM (memory)
d. None of the above

The correct answer is c.
Hardware (layer one) includes CPU, motherboard, and RAM.

Which of the following could be found in the operating system layer?

a. Google Chrome, Internet Explorer, Microsoft Office
b. Linux, Windows, or macOS
c. CPU, motherboard, RAM (memory)
d. None of the above

The correct answer is b.
Operating Systems (layer two) could include Linux, Windows, or macOS.

Which of the following could be found in the applications layer?

a. Google Chrome, Internet Explorer, Microsoft Office
b. Linux, Windows, or macOS
c. CPU, motherboard, RAM (memory)
d. None of the above

The correct answer is a.
Applications (layer three) could include Google Chrome, Internet Explorer, and Microsoft Office.

If your monitor turns on, yet it displays "the blue screen of death," what layer is associated with this issue? Remember, it occurs when you power your system on.

a. Applications
b. Operating system
c. Hardware

The correct answer is b.
The operating system or more specifically, the BIOS (basic input/output system), AKA system set-up, is the program a computer's processor uses to get the system started when powered on. If you see a blue screen of death, it's most likely due to an operating system issue.

Module 2 Cyber Visualization

Close your eyes… no really, close them… and imagine a world without the internet. It's hard to do. Technology has advanced greatly since its inception, and much of it is due to virtualization and a software technology called a hypervisor. Once upon a time in a far away place called the '80s, the three layers of the computer operated as one unit. If the O/S on your computer was Linux and you wanted to add Windows…you would have to buy a new computer. Could you

access your email from various places - not just work? Not a chance. In the ‘80s, people had to drive into work simply to access their email! Computing, as we know it today, would not be feasible if it were not for virtualization. Virtualization allowed the applications, O/S, and hardware to “separate” and operate within their own compartment.

Then, with the invention of the internet, these computers were able to communicate across long distances. Companies capitalized on these new technologies by offering services that allowed you to securely access and store your data away from your computer…launching the “formation” of clouds. How can we better understand the concept of “clouds”? Think about your utilities. Unless you’re Disney, more than likely you do not own a utilities grid—either you can’t afford one or it simply is not feasible. Yet, there are companies that can support this operation. So, you sign up with that company, use its services, and they bill you for what you’ve used.

Video: How it Works: Cloud Security (IBM Think Academy)

Begin Video Script.
Narrator: Cloud computing is transforming the way we do business, making I.T. more efficient and cost-effective, but it's also opening companies up to new types of cyber threats. Today, it's not a matter of if but when.

Mary is going on a cruise and notices the cruise line's website offers an image-sharing mobile application that is hosted on a cloud. The app will let her access her itinerary, track her trip, and share her vacation images with friends over social networks. However, after a week on-board, Mary begins to feel a little uneasy, and it's not seasickness. Many of her friends have complained to her that they were spammed after viewing photos she shared via the cruise line app. She complains to the cruise director. Meanwhile, back on shore, the cruise line's development team is already aware of the problem and is working to rectify it. So how could a cruise line know about this type of breach before the users themselves are aware, and what measures can they take to both alleviate any current problems and prevent them from happening again? The best defense?

A security incident response team that can quickly take whatever steps are needed to thwart attacks and restore system health. This team is on point to guard the cloud, armed with the latest software and security technology. They can tackle the full gamut of security issues through three important steps: monitoring data, gaining visibility in the cloud, and managing access.

Let's look at monitoring data. Danielle is the cruise line's data security analyst. Her cloud data activity monitoring system notifies her that there's something fishy going on, but the system doesn't just flag a set list of threats. It can detect new types of possible security threats. It uses advanced machine learning techniques to build detailed models of normal system behavior and flags any deviations to these models, assessing the risk in each deviation. This, combined with built-in insights around known hacking techniques, enables the system to rapidly detect unusual user and database activity.

Danielle goes to Ian, the enterprise security analyst. Ian is able to provide her with the detail needed to gain visibility in the cloud. He monitors all the traffic going in and out of the cloud, using a variety of sophisticated software or virtualized software appliances. It detects multiple

suspicious events we call offenses. All this activity is collected and analyzed within the cloud to work out not only what is happening but who is responsible for the offense. The system basically looks for patterns. It will correlate perhaps millions of events as it searches for suspicious patterns, patterns that deviate significantly from normal system behavior. It provides the visibility to quickly pinpoint and identify the hacker's credentials. In this case, Ian and Danielle quickly realize that a group of hackers has compromised a team member's password and used it to access the cloud management console. From there, they were able to create unauthorized administrator accounts, which then introduced the malware that created the spam. To address this issue, the incident response team can remove the new administrator roles created by the hackers and change all cloud credentials and passwords.

These measures thwart the hackers' malicious activity by shutting down their privileged access. To prevent further cloud breaches, Ian finally talks to Annika, the identity and access architect. Annika's job is to manage access. She uses a privileged identity management system, or P.I.M., that controls access to the critical cloud resources that store confidential and sensitive information. The P.I.M. uses a method of checking fresh credentials in and out each time the system that Annika manages is accessed. This adds an extra layer of security for users who have the high level of access to this confidential information. All of these steps are crucial, particularly when you consider that a typical organization has seven hundred eighty-five different cloud applications in use, but surprisingly, on average, they only know about sixty of them. The rest of the apps are unknown and unsanctioned. Security is a journey, not a destination. Security intelligence monitors data, gains visibility, and manages access in order to evolve and respond to the ever-changing world of the cloud.
End Video Script.

Now, transfer that concept to your computer and the cloud. It is quite costly to operate a data operations server room (e.g., equipment, building, etc.) So, there are companies that will offer IaaS (Infrastructure as a Service) and will support firms for a fee. Some firms cannot support their own databases, so, PaaS (Platform as a Service) will support that and more. But now, let’s make this a bit more personal: the internet. More than likely, you could not build and maintain the necessary equipment needed to link into the internet to access email, YouTube, games, etc. Therefore, you sign up with an internet provider company (e.g., Verizon, DirecTV) that can provide access to SaaS (Software as a Service) services for a fee.

Does the government use cloud services? Yes, the government does use cloud services with closely-controlled access for government employees and affiliates. Many of these cloud services are set up as private clouds, which are dedicated exclusively to one organization and are not on the internet. When using cloud services, we are trusting others with our sensitive and valuable data. These services have vulnerabilities and limitations.

Reliability and Availability of Service. We expect our cloud services and applications to always be available when we need them, which is one of the reasons for moving to the Cloud. But this isn’t always the case…especially in severe storms that cause power outages.
The Cloud Service Providers (CSPs) have internal uninterrupted power supplies, but even those can sometimes fail…so we can’t rely on cloud services to be up and running 100% of the time.

Using a cloud service means we're also dependent on the internet, which can be impacted by weather and maintenance. How long could your office go without having access to files and applications?

Data Protection and Portability: When choosing to switch from one cloud provider to another, we have to address the problem of data movement and deletion. The old CSP must delete all the data we stored in its data center. Alternatively, if a CSP goes out of business, they must provide the data to the customers, so they can move to an alternate CSP, after which the data must be deleted. Since we are on the subject of the internet, let's take a few moments to discuss how that system networks and communicates.

Why do you need to understand networking and communication? Many of the cyber threats discussed in our field stem from some vulnerability within these areas. These darn breaches! Will they ever go away? They have been a "wake-up" call for our community. The solution is encryption. When we use the internet, we're not always "surfing." Many times we're ordering something or setting up an online account. Most likely, we're doing something requiring us to enter a good deal of sensitive personal information.

Encryption is the process of encoding information in such a way that only the person (or computer) with the key can decode it.

Video: What is Cartography? (YouTube Channel: Learn Math Tutorials)
Begin Video Script.
Paul: Hey, everybody, this is Paul. Welcome to your first lesson in cryptography. So to explain what cryptography is, I'm just going to start out with a little example. So let's say that we've got some person. So let's just go ahead and name this person Paul since that's a pretty neat name. And then let's say that Paul has a friend. Let's pretend like Paul and his friend are on different sides of the world, but Paul has an important message to send his friend. But because Paul is on the other side of the world, he can't just hand his friend this message. So now let's pretend like this message that Paul has some secret information that he only wants his friend to know about and nobody else. Well, if Paul sends his letter to the friend around the world, there's going to be a whole bunch of people that will be handling this letter. So there's a risk that as Paul sends this letter, somewhere along the way, the letter may be intercepted by somebody other than Paul's friend. And if this letter falls into the hands of the wrong person, that person may read the secret message. Sometimes that person will keep the message, or he could take note of that information and then continue to pass the letter on to Paul's friend.

So how can Paul and his friend be sure that nobody in between has uncovered the secret message. One thing Paul could do is he could use cryptography to encrypt the message. That way, if somebody in the middle got the message, they would be unable to understand its contents. So when Paul first writes the letter, he writes it in English because that's the language he speaks. So if Paul wrote his letter in English, Spanish, Chinese, German, French, or any of the common languages that a multitude of people understand, we would consider that this message is written in plaintext. So if the message is written in plaintext, that means it's very easy for anybody who speaks that language to understand its contents. So what Paul needs to do is he needs to encrypt his message before he sends it. So what does it mean to encrypt a message?

Let's pretend like Paul's secret message is the word "fun." He doesn't want anybody other than his friend to read this secret message. Well, anybody that speaks English can read the letters f-u-n and understand that Paul is trying to send the message "fun" to his friend. So in order for Paul to encrypt the plaintext "fun," he converts the letters f-u-n to numbers. Then once his message is in numerical form, he can use a key to modify the values of this number. You can think of the key as mathematical operations that we can perform on the numerical value of Paul's message. After applying the key to this numerical value, we end up with a new numerical value, which is known as ciphertext. So now if Paul puts his ciphertext in an envelope and sends the envelope to his friend, Paul won't have to worry about somebody in the middle discovering the secret message. If somebody in the middle discovers the message, they won't be able to decrypt the message without a proper key. Now if the message continues to Paul's friend, Paul's friend will need a way to decrypt the message and recover the original plaintext. So in order to convert the ciphertext into plaintext, Paul's friend needs to decrypt the ciphertext. In order to decrypt the ciphertext, the friend will need a decryption key. Using the decryption key, the friend will be able to convert the ciphertext into the numerical value corresponding to the plaintext. Once the friend has the plaintext value, he can convert it back into the original message. Now that the numerical value is converted back to the English language, the friend has retrieved the original plaintext that was sent in Paul's message. So in a nutshell, that's how cryptography works.
End Video Script.

Computer encryption is based on the science of cryptography. Without cryptographic network security protocols, internet functions such as e-commerce would not be possible.

Secure communication is necessary because attackers try to eavesdrop on communications, modify messages in transit, and hijack exchanges between systems. Some of the tasks network security protocols are commonly used for are: file transfers, web communication, and Virtual Private Networks (VPNs.)

File Transfer Protocol (FTP) is the most common method of transferring files. A problem with FTP is that it sends files in cleartext, meaning it is unencrypted, and, therefore in a form that others can compromise. For example, many webmasters update their sites using FTP; an attacker using a packet sniffer and the website’s IP address can intercept all communications between the webmaster and the site’s server.

As an alternative…Secure File Transfer Protocol (SFTP) offers a more secure way to transfer files. SFTP is built upon Secure Shell (SSH) and is able to encrypt commands and data transfers over a network, thereby reducing the likelihood of interception attacks. The SSH cryptographic protocol is also resilient to impersonation attacks, because the client and server are authenticated using digital certificates.

A Virtual Private Network (VPN) creates an encrypted connection over a less secure network, such as a public WiFi Hotspot or the internet. Often, businesses use them to enable employees to securely access sensitive data.

Module 2 Knowledge Check

Use your knowledge of virtualizations, Clouds, and encryption to select the best answer. Then click the arrow for the next question.

This allows the three layers of a computer to “separate” and operate within their own compartment.

a. Virtualization
b. Encryption
c. Virtual Private Network

The correct answer is a.
Virtualization allows the three layers to “separate” and operate within their own compartment.

This creates an encrypted connection over a less secure network such as a public WiFi Hotspot or the internet.

a. Virtualization
b. Encryption
c. Virtual Private Network

The correct answer is c.
A Virtual Private Network (VPN) creates an encrypted connection over a less secure network such as a public WiFi Hotspot or the internet. Often businesses use them to enable employees to securely access sensitive data.

This is the process of encoding information in such a way that only the person (or computer) with the key can decode it.

a. Virtualization
b. Encryption
c. Virtual Private Network

The correct answer is b.
Encryption is the process of encoding information in such a way that only the person (or computer) with the key can decode it.

Module 3 Cyber Security Protection

Hacking techniques are often utilized by our foreign adversaries. They use the same skills and techniques used by freelance hackers. In order to protect our systems, it’s important to understand their methods. So, how do hackers break in?

Unlike in movies where hackers break into a computer in minutes with only a few key strokes, hacking deep enough into a computer to take control of it might take days or weeks. Hackers follow a set of procedures that are designed to pry open a crack wider and wider with each step.

Sophisticated hackers perform a footprint analyses of the intended target by using publicly available information, such as size, subsidiaries, and vendors that might have access to the target’s computers. Using readily available hacking software, hackers scan the target’s computer ports for potential break-in points (Remember ports from an earlier module?). Ports are numbers used to identify different services the computer provides, such as email and web browsers.

Second, based on the feedback, hackers create a map of the ports and their relationships to each other. Hackers use this to try to identify the types of file transfer and email the system uses by sending random data to the ports. Many port services respond to data with a banner that identifies the software that's using the port. Hackers look up the software in online databases that list the software's vulnerabilities. Some ports yield real pay dirt in the forms of usernames and dates that passwords changed.

To gain access to the target system, hackers have two approaches. The low-tech method involves contacting employees to trick them into revealing their passwords. Hackers may call pretending to be part of the IT help team. But in our environment, the method used is brute force attack. Hackers use a hacking program to try to log onto the system with the usernames acquired. When the system asks for a password, the program responds with a word from a list of likely passwords (e.g., opensesame, or 12345). The program repeats the process until the list is exhausted, it chances upon the right password, or the host locks the user out for too many failed attempts.

After hackers have entered the system with the user-level privilege, they look for passwords of high-level users that grant greater access to the system. Finally, with access to the most secret ranges of the network, hackers upload Trojan programs to one or more of the computers on the network. These programs appear to the human eye or a virus scanner to be ordinary, harmless files. In actuality, they are programs that open a backdoor through which the hacker may now enter the network at will.

So, how do we protect our systems against these attackers? Though security can be complex and overlap in many areas, let's categorize security in three layers: Firewalls for your hardware, firewalls and antivirus programs for your O/S, and encryption for your applications.

Remember, it's not enough to simply deploy these protocols; they must be maintained and remain in compliance to ensure that risks are managed. Firewalls offer protection for both the Hardware and O/S. In the case of the hardware, this functionality is built into the internet router. Both types are designed to block a hacker's attempts to break into a computer or network.

A firewall manager sets up rules the firewall uses to filter unwanted intrusions from the internet. The wall shuts any non-essential ports a hacker might probe for openings. The firewall manager might block all inbound traffic except for email or data that someone inside the firewall has requested.

Packet filtering is one technique, among many, for implementing security firewalls. Data such as email, web pages, and graphics travel over the internet and into a computer in the form of packets, or small chucks of data, that include addressing information about where the data originated and where it's bound. A packet is very much like a letter in an envelope. The data is the actual letter sealed inside the envelope and only can be accessed by those who are authorized to see it. Meanwhile, the address on the outside of the envelope is viewable by everyone. Otherwise, how would the post office know where to send the letter? The packet filter is the postal worker. It examines the packet's addressing and if the outbound address of the data is on a

list of banned internet locations, the firewall blocks it. However, the packet filter does not open the packet and read the data held within.

All traffic in or out of the network goes through a file server called a proxy, located outside the firewall. The server examines all data based on the packet filtering rules and only forwards packets that obey the rules. If a dangerous transmission manages to sneak past the filters, the proxy intercepts to protect the network.

The firewall inspects the packet. If suspicious activity is detected, it sends an alert in the form of a pop-up window or email to notify the computer's user or network manager that someone might have tried to break in. Antivirus, or antivirus software, sometimes known as anti-malware software, is computer software used to prevent, detect, and remove malicious software.

Antivirus software was originally developed to detect and remove computer viruses, hence the name. However, with the proliferation of other kinds of malware, antivirus software started to provide protection from other computer threats. In particular, modern antivirus software can also protect from many types of malicious code.

Zero-day threats are attacks that use an unknown exploit/attack for which no patch or antivirus definition file exists as yet. To mitigate the risk of a zero-day, administrators ensure that all patches are up to date to limit the scope of a potential attack. The second option is to use a good antivirus solution. A zero-day attack does not become public knowledge for a period of time and during that period, the antivirus program will not detect any file containing this specific vulnerability by using standard pattern analysis techniques.

Antivirus software runs in the background on your computer, checking every file you open. When you double-click an EXE file, it may seem like the program launches immediately – but it doesn't. Your antivirus software checks the program first, comparing it to known viruses, worms, and other types of malware. Antivirus programs also scan other types of files that can contain viruses. For example, a .zip archive file may contain compressed viruses, or a Word document can contain a malicious macro. Antivirus software scans files whenever they're used – for example, if you download an EXE file, it will be scanned immediately, before you even open it. Encryption provides protection for data susceptible to eavesdropping attacks, password crackers, or manipulation.

Almost every company has transactions, which, if viewed by an eavesdropper, could have negative consequences. Encryption ensures that when sensitive data passes over a medium susceptible to eavesdropping, it cannot be altered or observed. Decryption is necessary when the data reaches the router or other termination device on the far-reaching Local Area Network (LAN) where the destination host resides.

Most encryption algorithms can be broken, and the information can be revealed, if the attacker has enough time, desire, and resources. A realistic goal of encryption is to make obtaining the information too work-intensive to be worth it to the attacker.

Video: Cybersecurity 101 (PBS NovaLabs)

Begin Video Script.

Narrator: Would you be comfortable living in a house that someone else had the key to? What if an underground tunnel led into it from a public park, or its windows could never quite close all the way? Would you trust it with your safety and your privacy?
The internet is that house. This is not to say—never go into the house, but rather, you should know the hazards before you store all of your valuables there—and do what you can to protect them.

So why is it insecure, and why can't we just fortify it until it's safe?
Well, first of all, the internet was not originally built to be what it is today. It's like someone decided to expand a shoebox into a skyscraper. The internet originally developed when computers were huge and so expensive to own that only universities, big businesses, and a few governments had them. The point, originally, was to let these massive supercomputers talk to each other. And as soon as two computers could send information back and forth, we had a network. The network gradually grew, until personal computers emerged in the 1980s, and then it exploded.

Soon people were not just talking to each other, but also exchanging money, playing games, reading news, shopping, and doing everything we associate with the internet today. Other devices started talking to the network too—phones, and cars, and refrigerators, and elevators and power plants, and much much more.
But the ease of all of those devices talking to each other came at a price: security. One computer could send another instructions to delete everything on it or take it over—we call these viruses and malware. Or one person could steal another's identity by guessing, cracking, or extracting a password.

Vulnerabilities such as these will never completely go away, because they're built into the internet's very architecture. Criminals use them to steal billions of dollars, governments use them for surveillance, and hacktivists use them to further their political goals. Between 2004 and 2013, over 1 billion records of personal information were stolen or leaked through data breaches of major organizations.

As a thought experiment, let's imagine what a perfectly secure internet might look like. Users would not be allowed to download or install anything onto their computers. All internet traffic would be monitored and regulated by bots and humans, massively limiting the number of websites you could visit. In order to log onto a website you'd have to type in a 100 character password, submit a genetic sample, and whistle a tune.
The servers that hold data would be kept in heavily armed fortresses... on the moon. And even with all of these safeguards in place, some clever hacker would almost certainly still find a way in.

The good news is, even with our flawed internet, there are simple things you can do to protect yourself, and there are a lot of people committed to making the internet more secure.

In NOVA's Cybersecurity Lab, you'll play as one of these people, protecting a company that is the target of increasingly sophisticated cyber attacks. You must continuously strengthen your defenses in order to thwart these attackers. You will do this by completing challenges that will give you basic coding abilities, help you spot scams designed to trick you into giving up your secrets, and teach you how passwords are cracked and strengthened.

The house that is the internet may be built on a shaky foundation, but it's been a home to innovation and an unprecedented free exchange of ideas. It's up to us to make it livable in spite of its flaws.
End Video Script.

Module 3 Knowledge Check
Use your knowledge of the protection protocols and their associated layers to select the best answer. Then click the arrow for the next question.

Which protocols should you apply to protect your hardware?

a. Encryption
b. Antivirus and firewalls
c. Firewalls

The correct answer is c.
Firewalls built into internet routers protect hardware.

Which protocols should you apply to protect your Operating System?

a. Encryption
b. Antivirus and firewalls
c. Firewalls

The correct answer is b.
Antivirus software and firewalls protect the operating systems. Antivirus software prevents, detects, and removes malicious content and firewalls block a hacker's attempts to break into a computer or network.

Which protocols should you apply to protect your applications?

a. Encryption
b. Antivirus and firewalls
c. Firewalls

The correct answer is a.
Encryption protects applications and the data susceptible to eavesdropping attacks, password crackers, or manipulation.

Remember, it's not enough to simply deploy these protocols; they must be maintained and remain in compliance to ensure that risks are managed.

Congratulations! You have completed the Cyber Explore: Fundamentals of Cyber course.

You now know that foreign adversaries could infiltrate and exploit our cyber networks through inherent and/or self-imposed vulnerabilities and the security procedures you can implement to help mitigate the risk.

Join us for the other courses in this cyber series where we will further explore the threats inherent in the cyber realm and learn more about how to secure information systems and data. Click here to download your certificate.