Cyber Aware: Anatomy of a Hack

Introduction

On-screen Text

The more you know…

Awareness leads to action.

It's time to buckle up!

Host Video - Connecting to IT

Oh! Hi!

Get this; You've probably witnessed this scene before… the Hollywood hacker sits in front of a computer typing frantically, and breaks into this top secret system in less than a minute. Well, it's a bit more complicated than that. There's prep work and a process to follow… It all depends on the skill set of the hacker, and the type of data the hacker is trying to obtain, but this stuff is real. No kidding.

So, I heard you're going through a series of cyber courses. Good. It's needed, and it will make my job a lot easier. So, what did you learn? All about hardware? Operating systems? Applications? Vulnerabilities that lie within networks and counter security measures? It's a lot to take in, I know… but welcome to my world. Now that you understand what I go through every day… maybe you'll ease up on me a bit, right? Right.

I hope you've learned a lot – but here's your big take-away… the protection of data from hackers is critically important, and is two-fold process: The back-end process that IT folks like me are responsible for, and the front-end part that you, and every other computer and network user, can do to help lessen the risk.

Got a minute? Step into my world and see what happens behind the scenes and how you can help stop hackers. Let's go!

Onscreen Text

Big takeaway…the protection of data from hackers is critically important, and is a two-fold process:

1. The back-end process, the IT department's responsibility…
2. and the front-end part, what users can do to help lessen the risk.

Cyber Aware: Anatomy of a Hack

Facts

- 80% of cybercrimes are generated by highly organized criminal gangs.
- The average age of a cyber criminal is 35.
- 63% of confirmed data breaches involved leveraging weak/default/stolen passwords.

Onscreen Text

This course provides an introduction to methods that hackers might use to access a computer system or network. It also provides insight into how users like yourself can make the adversary's job more difficult.

Let's Go

Select a module below to continue.

Earn your certificate by completing the Experience activities.

01 Learn

Learn about hackers and their motivations.

02 Experience

Experience a cyber intrusion from the adversary's perspective.

03 Examine

Explore real-world intrusions and data breaches.

Cyber Aware: Anatomy of a Hack

Module 1 – Learn About Hackers

Host Video - Connecting to IT

What is hacking? Webster's Dictionary traditionally defines it as *"…cutting through something with rough, or heavy blows.*" And then about 20 years ago, they added a computer reference --*"using a computer to gain unauthorized access to data in a system."* Yup. That's the one we're talking about.

On-Screen Text

There are 3 types of hackers: black hats, white hats, and gray hats.

Black hats are the bad guys. They're criminals that use their skills to break into computers or networks and steal data. They may sell malicious code or the stolen data to other criminals.

White hats, a.k.a. ethical hackers, are security researchers or hackers who work for organizations or software vendors. They find vulnerabilities in order to develop patches that mitigate the risk.

Gray hats look for vulnerabilities within a system without permission. Unlike black hats, they don't use the vulnerabilities they find for illegal purposes. They sell or disclose the information to governments, law enforcement, intelligence agencies, or military organizations. They may also report the find to the owner and offer to fix it for a small fee.

Host Video - Connecting to IT

Okay, the million-dollar question: Why hack?

For a bad guy: why not? It's big business, and there's often money to be made by selling ill-gotten gains on a secretive part of the internet known as the dark web. As discussed in the Cyber Explore course, from a counterintelligence point of view, some nation-states even hack to improve their country's standing or to cause harm to another.

On-Screen Text

Today's hackers: who they are, what they do, and why they do it.

Nation-states

Nation-states include foreign government military and intelligence units. Nation-states and state-sponsored hackers are usually well-resourced. Those working on behalf of a foreign government, but aren't employed by them, are considered state-sponsored.

They may manipulate, degrade, or destroy data and/or infrastructure within a targeted network in order to gain state secrets, weaken national security, or improve their country's economic edge.

Organized Crime

Criminals operate within the cyber realm for monetary benefit. They employ many different schemes to generate profit. Technology enables a greater reach with less risk and danger than traditional criminal pursuits.

Terrorists

In the cyber realm, terrorists could attempt to disrupt large-scale computer networks, potentially interrupting critical infrastructure or financial systems. Terrorists systematically use or threaten to use violence to create a general climate of fear in a population with the intent of furthering their political or ideological goals.

Hacktivists

Hacktivists blend activism with hacking and seek to disrupt services and bring attention to a political or social cause.

Insiders

Insiders are individuals who already have access to an organization's network who decide to obtain and exploit information for personal gain.

Host Video - Connecting to IT

Think about this: Once the breach has occurred, it's too late – the damage is done, or at least begun. That's why, with the recent successes of so many cyber-attacks, security experts now conclude that the best approach is to be proactive and to take action before the attack occurs.

Let's not get too far ahead of ourselves, though… You need to understand what hackers actually do in order to gain access to our systems. We're going to expose you to one of the most common processes and methods used to infiltrate networks and entire IT systems, and how you can be part of the digital army needed to stop them.

Cyber Aware: Anatomy of a Hack

Module 2 – Experience a Hack

Host Video - Connecting to IT

Oh! Hey! There you are. Welcome to "Experience." In this module, we'll look at a cyber intrusion from the hacker's perspective.

First, the disclaimer: we're simplifying things quite a bit. You won't learn how to hack here. What you'll see below is meant to show you how hackers operate so you can be better prepared. Oh, and don't try this at home.

On-screen Text

Let's start with an analogy. Imagine a burglar wants to break into your house. He does some research—he cases the place. He observes who comes and goes from the house, your schedule, and your habits. You typically lock your doors and windows, but the burglar will check to see if you left your basement window open.

Evan better, let's say this is a new house. The burglar might see that you installed an alarm system. So, now this burglar can go online to see the vendors that work with your builder to determine the alarm system brand. Once he has the brand, he can find its vulnerabilities and so forth.

Now let's apply the same concepts to how a hacker might operate. Before doing anything, the hacker determines his mission and objectives. Remember the goal could be to steal secrets and intellectual property or disrupt or destroy networks or information.

Now he begins casing the company and its computer networks—known as footprint analysis—which will help him determine the best way to go about getting the prize.

First, the hacker researches all potentially related company information such as size, subsidiaries, vendors, and customers, as well as individual employees and affiliates that might have access to the target's computers. Remember, the easiest way into a system may be the long way around—through a third party.

Much of this information is publicly available. The Intelligence Community refers to publicly available information as open source intelligence (OSINT). The hacker conducts online research, viewing news organization, social, media, job search, and company websites.

He'll also want to know the Internet Protocol (IP) addresses associated with his target. For many companies, he'll be able to look-up an IP address by knowing the company website address or domain name. Knowing the IP address will help the hacker infiltrate the network. You'll see how they come into play when we move into port scanning.

Cyber Aware: Anatomy of a Hack

The adversary may also use old-school techniques:

- eavesdropping
- dumpster diving
- observing

All of these tidbits are used to identify vulnerabilities and potential human targets of a social engineering-based intrusion.

Social Engineering is a broad definition referring to using deceitful techniques designed to manipulate someone into divulging information or performing actions that may result in the release of that information.

The low-tech method…someone claiming to be calling from a help desk tricks a user into revealing their username and password.

Phishing uses email in an attempt to get people to reveal sensitive information or unwittingly install malicious code. In this example, an email that looks like it's from the help desk, is really from a hacker. The email instructs the user to download and install an update, but the file contains malicious code.

Here’s your chance. Click the start button below for your chance to experience a cyber intrusion from the hacker's perspective.

Want to review the activity steps? Click Close (X) to return to the activity menu.

View an animated demonstration of what might happen behind the scenes of a hack.

As you move through the experience, the videos will provide context and direction.

Complete the activity here when prompted. Click Reset Experience to review the activity again.

Exercise 1 | Footprint Analysis Researching

Host Video - Connecting to IT

The internet is a treasure trove of information. From a simple internet search, the adversary can create an in-depth picture of a business and identify potential vulnerabilities.

Websites are often created to advertise a company's capabilities or gain clients. So, how could that be bad? Let's take a look…

The QX9 Group website indicates that the company is an innovator in information technology and data analysis solutions, and they're a defense contractor. The information they've provided could easily make them a primary target or enable the adversary access to a government system.

Scroll through the types of information to reveal how the information may help the hacker and where the information may be found.

On-Screen Text

Directions: Scroll through the types of information to reveal how the data may help the hacker and where the information may be found.

Leadership (or employee lists) may provide a starting point for the adversary's research.

Host Video - Connecting to IT

What's the harm in highlighting the names of leadership or key employees? The fact is, this is often a good starting point for the adversary's research. It's a string to pull. From a name, an adversary can possibly gather details such as information on friends, family, hobbies, and associations – all of which can be used for social engineering.

On-Screen Text

Job postings reveal critical shortfalls, technology/projects.

Host Video - Connecting to IT

Everyone lists jobs, so what? Job postings can reveal critical shortages or indicate the types of technology being used or current and future projects along with project names.

On-Screen Text

Press releases include client names, technology, and projects.

Host Video - Connecting to IT

Press releases are vital communications tools for companies – right? Well, they are but they're also a source of information for the adversary. Press releases often contain client, technology, and project information. In this case, the press release provides a possible social engineering target for the adversary, Diane Johnson, an unsuspecting and trusting new employee.

On-Screen Text

Publications list areas of expertise, past work, and names of experts.

Host Video - Connecting to IT

It's exciting to get published but what are you really saying? Just like job postings, professional papers could give insight into a company's or individual's technology focus and accomplishments. If an adversary is interested in intellectual property or the types of technology for future government tech efforts, you've just provided them with extremely valuable research materials!

On-Screen Text

Domain look-up sites list IP addresses that will be targeted

Host Video - Connecting to IT

You might be thinking that a domain name, web address, website, and IP address are all the same thing; they're not. A domain name is a registered web address. Websites are located AT a web address. In this case, www.QX9Group.com is the domain name and a registered web address. The website displays as the web address. A domain name can exist even if a website isn't built. Have you ever hit a site that just says under construction? That's a domain without a website. An IP address is a unique string of numbers that traces back to a specific device. Why does this matter? The information is being addressed is gold to a hacker. With these details, he can attempt to target devices to gain access to a company's network.

These are just a few ways that an adversary can hack and steal information and conduct malicious activities. Check out some other potential nuggets of information.

On-Screen Text

There are many types of information that can be gleaned from the internet. Information can increase the adversary's understanding of an organization, help identify weaknesses, and also identify information to use in social engineering attacks or to identify penitential targets for social engineering. Information that seems harmless may aid the adversary:

- Organization's address can be used for physical surveillance or dumpster diving.

- Hours of operation indicates times of minimum manning or maximum activity.
- Business social media accounts list new employees and upcoming events. They may reveal social engineering opportunities.
- Personal social media account include travel details, lists family members, and indicate hobbies or interests.
- Job listing sites may reveal critical voids, skills sets needed for technology or projects. They may also provide the adversary with a way to gain access to a facility as an applicant or new hire.
- Resume sites list past clients, projects, technology, skill sets. They can be used to identify a current employee seeking a new job or a past employee. Both may be targets for social engineering or their names and information may be used within a social engineering scheme.

How can we protect our information? Many organizations have a policy for social media channels, websites, and press releases. Someone might even review content from an Operations Security (OPSEC) perspective before it's shared online.

It's a fine balance between information protection and sharing. You might want to share in generalities and leave out the specifics.

We all have a responsibility to protect critical information, so if you see something that might help the adversary, bring it to the attention of someone who can help.

Exercise 2 | Footprint Analysis: Port Scanning

On-Screen Text

The hacker's footprint analysis continues with port scanning IP addresses. In computer networking, a port refers to the digital conduit through which network devices process information from the internet or other devices. Each port is assigned a number (port 25, port 80, port 443). The numbers are used to determine what kinds of information are being sent or received. Think back to our house analogy–Ports are like the doors and windows.

Remember, the hacker learned the IP address from a domain look-up site (www.QX9group.com). The hacker then:

- Uses software to scan for open ports on the network–places he might be able to break in.
- Sends random data to the ports, so he can identify the type of file transfer protocols and email software that the system uses. Many port services respond to data with a banner that identifies the software that's using the port. Exploiting this information is called banner grabbing.
- Looks up the software in online databases that list the software's known vulnerabilities. Now he knows the software being used and its weak points.

All software has vulnerabilities. Software companies are forever creating and sending patches to address newly discovered issues. However, if a company or individual doesn't install those patches or the software has known unaddressed vulnerabilities, the adversary can use malicious code to leverage these vulnerabilities. These security gaps are why it's so important to keep your operating system and all software up to date. Based on this analysis, the hacker creates a map of the ports and their relationship to each other.

Host Video - Connecting to IT

To scan for open ports, the hacker can run scanning software on the IP address that he found on the IP look-up site to find a port to target.

Type in the IP address, then click to run the scanning software.

Directions: Type in the IP address: 10.10.10.143 then click the Run button to launch the scanning software.

The response indicates that port seventy-one fifty-one is open.

Now, he wants to identify the software and version to determine if and how to exploit it.

The hacker would use some code or a tool. To simplify this for our purposes, enter the IP address and then the port number and type "GET."

This returns the banner, which includes the type and version of software using this port. This is called banner grabbing. Abso-DB 4.4.3 is running on port seventy-one fifty-one. Good news for the hacker because this database permits remote connection.

A quick cross reference tells us that this is an old version, and it had an admin password hardcoded. Meaning that any user who is aware of the vulnerability and knows how to exploit it can gain admin privileges within the database. QX9 Group should have installed the patches to update the software to the current version, Abso-DB 4.5.0, and protected themselves from this vulnerability.

On-Screen Text

Can we do anything about port scanning?

Open ports are vulnerabilities. Good guys can use the same techniques as bad guys to identify these vulnerabilities: red teaming, ethical hacking, white hat hacking.

IT professionals perform port scans to determine system vulnerabilities and then restrict access to servers and shut down unused or unnecessary services.

Cyber Aware: Anatomy of a Hack

Exercise 3 | Gaining Access

On-Screen Text

The hacker has identified a vulnerability within the software being used by the target, so he can choose malicious code to exploit the vulnerability. He may have identified specific employees for a social engineering approach to enable him initial access to the network.

Host Video - Connecting to IT

From the open source research, the hacker determined that Diane Johnson would be a good target for a phishing attack. She's new and may be less likely to question an email from IT. Given her role in supporting technology integration, she might even have access beyond the regular user.

The hacker will ask Diane to change her password on a Friday afternoon before a holiday. Take a look – the email looks legitimate and so does the password reset website. However, they are not; they're spoofs or copycats. Hackers create spoof websites and emails in order to trick people into revealing sensitive information.

Go ahead and click "Send" and see if she falls for it.

Ok, now Diane unknowingly gave the hacker her password.

On-Screen Text

Phishing attempts are why IT warns us not to click on suspicious links or file downloads and suggests that we verify requests for sensitive information. It's up to all of us to protect sensitive information.

- Usernames & passwords
- Accounts
- Financial information.

Another way to access a system is through a brute force attack. In Cyber Explore, we learned that brute force is a trial-and-error method used to obtain information such as a password or a PIN.

This technique uses automated software in an effort to try every possible password contained within a pre-defined dictionary.

Brute force attacks are why users are encouraged to use complex passwords containing a combination of special characters, numbers, and upper and lowercase letters. The more complex the password, the harder it is for a brute force attack to be successful.

Cyber Aware: Anatomy of a Hack

Exercise 4 Escalating Privileges

On-Screen Text

Once the hacker is in the system, he will attempt to escalate his privileges to the administrator or admin level. An admin typically has the authority to install software, change configuration settings, create accounts. A hacker with full admin privileges would have the keys to the kingdom.

If the adversary knows where to look, they may be able to find critical information. The hacker will poke around the system to see what there is to see. Sensitive files and information may be visible without much effort. For example, passwords might be stored in clear text in batch files. Essentially, if the adversary knows where to look, he may be able to find critical information. From his research, he also may be able to identify other users who have administrative privileges.

Host Video - Connecting to IT

While the employees of QX9 Group are enjoying a long weekend, the hacker will be busy tapping away at the keyboard and perusing the network.

Enter Diane Johnson's username and password and click the login button.

Now, use the hardcoded admin username and password to access Abso-DB.

This provides him access to all records within the database including technical specifications, contract information, program details, and names and resumes of those associated with projects. It's a gold mine for the adversary.

He could steal and sell QX9's intellectual property, their research and findings. He could use the information for a variety of nefarious activities -- shutting down the servers, stealing trade secrets, compromising personal identities, or accessing financial information. Maybe all of these…

On-Screen Text:

How do we thwart the adversary? For starters, IT personnel are encouraged to view their network from the adversary's perspective and verify that passwords are stored in a secure manner.

This is also why IT is very stingy with administrator privileges; more accounts may provide more opportunities for exploitation.

If IT has ensured that passwords and sensitive information are stored in a secure manner, the hacker is forced to use another method.

Unfortunately, there are many different techniques to escalate privileges such as introducing malicious code to do their dirty work. A virus could create fake identities with administrator privileges.

Cyber Aware: Anatomy of a Hack

Exercise 5 | Installing a Back Door

On-Screen Text

Although the hacker gained control of a system by gaining full administrative privileges, his stolen username and password could be deleted with server maintenance. As added insurance, he wants to create a way to come back with less work; he installs a backdoor.

This backdoor is often created by a Trojan (an innocently named file that contains malicious code) or another type of virus. The hacker wants to minimize suspicion, so the file is named such that it looks like it belongs, but maybe it's just installed in the wrong place.

Host Video - Connecting to IT

In order to install the backdoor, the hacker is going to package malicious code in a file that appears to be a patch.

Remember, this entire hack was in an effort to reach a goal or a target. This hacker did his research and his intermediate goal is QX9 Group's Virtualization Suite. He intends to access the virtualization suite source code and copy it to either look for vulnerabilities or introduce his own.

Go ahead and click on the install button to install the backdoor.

On-Screen Text:

The U.S. Government uses many different commercial off-the-shelf devices that are susceptible to malicious access like computers, printers, copiers, smart TVs, and cell phones.

Unfortunately, adversaries can insert hidden malicious functionality into the devices' software and firmware, such as a backdoor, before you even take possession of it.

That's why supply chain risk management (SCRM) is critical. SCRM aims to counter adversarial threats and mitigate risks to your sensitive information and assets.

Ensure that SCRM is integrated into your organization's existing risk management processes.

The hacker can enter through the backdoor on his terms and timeline. It may be months or even a year before he makes another move. Or he could be quietly stealing or destroying data all the time.

Maybe the compromised system wasn't even the final target. When the hacker completed the footprint analysis, he may have determined that a subsidiary or vendor may be the path of least resistance to the actual target.

This may be just the beginning.

Cyber Aware: Anatomy of a Hack

Module 2 Conclusion

Host Video - Connecting to IT

So, there you have it – Hacking 101. Like I said, we all have a part in keeping our information safe. Bewildered? Don't know where to start? It's not so hard. Use complex passwords. Be wary of unsolicited email. Think before posting on social media. And always follow your organization's acquisition and IT policy. It's there for a reason.

Click Examine to learn about real-life examples and don't forget to print your certificate.

Cyber Aware: Anatomy of a Hack

Module 3 – Examine Incidents

Real Life Examples

Now that you've experienced what a hack looks like, explore these real-world hacks to see what went wrong and what can be learned from them.

OPM Incident

Sensitive information and Social Security numbers for 21.5 million individuals, were stolen from the background investigation databases of the Office of Personnel Management.

The Office of Personnel Management (OPM) is the central human resources planner for the Federal Government. OPM is responsible for the successful management of human capital across every federal agency. OPM assists federal agencies in hiring new employees, providing investigative services for background checks, and creating training programs to develop tomorrow's leaders.

In what appeared to be a coordinated campaign to collect information on government employees, attackers stole the personnel files of 4.2 million former and current government employees and security clearance background investigation information on 21.5 million individuals. Additionally, fingerprint data for 5.6 million of these individuals was stolen. Background investigation information includes some of the most intimate and potentially embarrassing aspects of a person's life, including whether the applicant consulted with a healthcare professional regarding an emotional or mental health condition, used illegal drugs, abused alcohol, or experienced financial problems.

Attackers were able to access OPM systems due to poor security protocols. OPM lacked an effective managerial structure to implement reliable IT security policies and didn't comply with the agency's IT security program. Implementing multi-factor authentication for employees and contractors would have thwarted continued access to the system.

MARCH 2014

- The U.S. Department of Homeland Security's (DHS) United States Computer Emergency Response Team notified OPM's Computer Incident Response Team that a third party had reported data exfiltration from OPM's network.
- In an effort to better understand the threat posed by the hacker, OPM monitored the adversary's movements.
- During this time, the hacker removed manuals and other sensitive materials that provided a roadmap of OPM's IT environment and key users.

May 2014

- While OPM monitored the first hacker, a second hacker used a contractor's OPM credentials to log into the OPM system, install malware, and create a backdoor to the network.
- Two months later, OPM began monitoring the first hacker, concerned for the safety of security clearance background information. OPM kicked the first hacker off of the system, but was still unaware of the second hacker.

July 2014-March 2015

- Security clearance background files, personnel files, and fingerprint data were exfiltrated.

April 2015

- OPM became aware of the data breach and began an investigation to identify and isolate all malicious code.

"This is crown jewel material…a gold mine for a foreign intelligence service." Joel Brenner, former NSA Senior Counsel

"[OPM data] remains a treasure trove of information that is available to the Chinese until the people represented by the information age off. There's no fixing it." Michael Hayden, former Director of the CIA

Cyber Aware: Anatomy of a Hack

Sony Pictures Incident

Personal documents, records, and email were stolen and leaked to the public in an effort to force Sony Pictures Entertainment (SPE) to cancel the release of a controversial movie.

The Federal Bureau of Investigation attributed the attack on Sony Pictures Entertainment to North Korea. This attack erased everything stored on over 3,000 computers and 800 servers, leaked personal documents, records, and embarrassing email to the public and eventually forced SPE to cancel the release of a controversial movie.

A myriad of basic security practices may have provided better protection for SPE networks and files. Had SPE implemented these security practices, it could have prevented some of the unrestricted access and massive damage the hackers inflicted.

Two-factor authentication (2FA) would have provided another layer of protection. 2FA requires both a password and another piece of information, such as a card, fob, or biometric. This added security may not have completely thwarted the hackers, but it would have made it much more difficult. Instead, the hackers used administrative usernames and passwords to gain unfettered access to of SPE's entire network.

Files containing social security numbers and other personal information lacked password protection, and seven years of email messages languished on servers without encryption.

SEPTEMBER 2014

- Hackers gained access to SPE by tricking an employee into clicking a malicious email attachment.
- Sensitive information, including administrator usernames and passwords, was kept unprotected in spreadsheets and documents, enabling hackers to steal seven sets of administrator passwords. They mapped SPE's entire network, identifying critical files and planning the destruction of servers and computers.
- Hackers patiently exfiltrated chunks of data from different servers to multiple hacker-controlled locations, making the theft difficult to detect.

NOVEMBER 2014

- A group calling themselves The Guardians of Peace (GOP) locked SPE employees out of their computers and threatened to release sensitive information.
- Almost immediately, the hackers leaked unreleased films with other data to follow.

DECEMBER 2014

- Hackers released performance reports, medical records, criminal background checks, passport information, salary details, and thousands of embarrassing email messages.
- Hackers threatened family members of Sony employees and threatened a 9/11 style attack if SPE released the *The Interview*. North Korea called the film about two journalists

recruited by the CIA to assassinate North Korean leader Kim Jong-un an "act of terrorism."

- Eventually, *The Interview* was released to 300 theaters on Christmas day. The film was more widely distributed online for rent or purchase through Google Play, Xbox and a special Sony website.

In closing**,** State-sponsored cyber criminals present a valid threat, are usually well-funded, and are difficult to defeat, but SPE's lack of security allowed hackers to capitalize on inherent corporate-wide vulnerabilities.

Cyber Aware: Anatomy of a Hack

Home Depot Incident

Credit card information of 52 million shoppers was stolen via the retailer's self-checkout system.

Hours after compromised credit card information appeared for sale online, the U.S. Secret Service contacted Home Depot. Upon further investigation, Home Depot announced that 56 million customer credit and debit card accounts were stolen, along with 53 million customer email addresses.

The Home Depot attack had similar markings to a breach of Target's network, including entry into the network via a third-party username and password.

Had they implemented two-factor authentication (2FA), which requires another piece of information such as a card, fob, or biometric, they would have added another layer of protection. Home Depot also failed to update its security software; it was still using Symantec's 2007 Endpoint Protection 11, which should have been upgraded three years prior to the breach.

APRIL 2014

- Using credentials (username and password) from a third-party vendor, hackers gained access to the perimeter of Home Depot's network.
- Once in the network, the hackers exploited a zero-day vulnerability. This previously unknown weakness within Microsoft Windows enabled them to escalate privileges, move laterally through the network, and identify 7,500 self-checkout lanes.

JUNE 2014

- The hackers deployed custom-built malware on the self-checkout system that stole customer credit and debit card information and email addresses.
- Data was exfiltrated during business hours so as not to alert Home Depot's security team.

SEPTEMBER 2014

- Credit and debit card information was offered for sale on an online underground cyber-crime shop. The email addresses were presumed to be used in phishing schemes, attempts to trick recipients into revealing sensitive information.
- Later, the Secret Service notified Home Depot that they traced credit card numbers for sale back to Home Depot.

Conclusion

Congratulations! You have successfully completed the Cyber Aware: Anatomy of a Hack course.

You now know that the 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.