Cybersecurity Investigator 2

Minesweeper Cards & Map Diagram

Before the meeting, create a "minefield map" for Seniors to use in Step Five.

- **Option 1:** Use painter's tape to mark an 8x8 grid of squares.
- **Option 2:** If your meeting space has large tiles on the floor, use the tiles as boundaries for your squares.
- **Option 3:** If you're meeting outside, use sidewalk chalk to draw the grid.
- **Option 4:** If none of these options will work in your site, create a minefield map simply by placing the cards on the floor in the appropriate position.

Then, lay out the Minesweeper Cards following the instructions below:

1. Put the "START" card down, face-up, on the edge of the map.
2. Follow the "Minefield Map Diagram" to create a safe path for Seniors to follow by placing the SAFE cards, face down, on the grid. Put one card in each square.
3. You don't have to use all the SAFE cards. The path can be as complex as you want, with cards connecting sideways or diagonally.
4. Once you've laid out the SAFE path, fill in the rest of the grid with the remaining Minesweeper cards.

Minefield Map Diagram

M	S	M	M	M	S	M	S
S	M	M	M	S	M	M	M
S	S	S	D	M	S	M	M
M	M	M	S	M	D	M	S
M	M	D	M	S	M	S	M
S	M	M	S	S	M	M	S
D	M	S	M	S	M	D	M
S	START	S	M	M	S	S	S

M - Mine!

S - Safe

D - Defense

How many maps do I need? The ideal team size for this activity is about six people, but it can easily be done with more girls. If you have a large group, you might want to set up two different Minefield grids, or let different teams take turns going through the grid. If you have less than six girls, work as one team.

© 2019 GSUSA. All rights reserved. Not for commercial use. This material is proprietary to GSUSA and may be used, reproduced, distributed exclusively by GSUSA staff, councils, Girl Scout volunteers, service units and/or troops solely in connection with Girl Scouting.

SAFE!	SAFE!
SAFE!	SAFE!

SAFE!	SAFE!
SAFE!	SAFE!

SAFE!	SAFE!
SAFE!	SAFE!

SAFE!	SAFE!
SAFE!	SAFE!

SAFE!	SAFE!
SAFE!	SAFE!

SAFE!	SAFE!
SAFE!	SAFE!

Defense You hire a “white hat hacker” to find vulnerabilities in your organization’s networks, and then follow her recommendations for improving cybersecurity.	**Defense** You have a strong company policy of regularly backing up your corporate data. Even if you fall prey to a ransomware attack, you will still have access to your data.
Defense Your entire organization attends regular trainings on best practices in cybersecurity.	**Defense** You receive a suspicious email from one of your clients that has no text but just an attachment. You forward it to your IT department immediately without clicking on the link and successfully thwart a malware attack.

Defense

You receive an email that appears to be from your boss, asking you to email some sensitive documents. You decide to verify her identity by calling her up first and discover that the email was spoofed. Instead of releasing data, you instead warn the rest of your coworkers to be on the lookout for suspicious emails.

MINE!

You connect your work computer to an unsecured WiFi network at a hotel.

A hacker is able to see the emails that you are reading and replying to.

MINE!

Your password is 12345678.

A hacker can crack your password within a few seconds.

MINE!

You allow a sales representative to connect her flash drive to your computer so she can show you her sales presentation.

When she opens the file, she also downloads malware to your computer..

MINE!

Someone calls your office, pretending to be from a shipping company. She asks for the security code to the loading dock. You give it to her without verifying her identity.

She is now able to hack into your security system.

MINE!

You leave your computer unlocked while you run an errand.

While you are gone, a visitor is able to gain access to all of your company's files.

MINE!

Your anti-virus software is out of date.

Your computer is left unprotected from malware.

MINE!

You receive a link that appears to be from your boss, asking you to send a check to a person whose name you don't recognize. You do so.

You've just fallen victim to a phishing scam and have given hackers access to your corporate accounts.

MINE!

You receive an email from a coworker with no subject line, just an Excel spreadsheet entitled "Budget Projections." You download the attachment and unknowingly download malware along with it.

MINE!

You download an unsafe app to your work computer.

Someone uses that app to hack into your entire network.

MINE!

You give admin privileges to the company's network to an employee who has limited technological knowledge.

Because her account is able to bypass certain security controls, she is more apt to download malware.

MINE!

You share your password with a coworker so that she can access your files.

This also gives her access to your personal information! Either intentionally or unintentionally, she may share your information with malicious hackers!

MINE!

You keep forgetting to update your software.

Often software updates are designed to fix security bugs. Using out-of-date software leaves your system vulnerable to security threats.

MINE!

You use the same password for your email as you do for all other online accounts.

When one site is breached, all the others can be, too.

MINE!

You give all your employees, regardless of their status, access to the shared network drive that contains sensitive information.

One employee develops a grudge against your company and leaks your data.

MINE!

Your computers are so old that they cannot support the latest updates to software programs.

Without replacing your computers, you are unable to fix important bugs in the existing software, leaving your network vulnerable to hackers.

MINE!

You email a sensitive document to yourself so that you can work from home. However, your home network is unsecured.

A hacker now is able to gain access to that document, and all of the sensitive data it contains.

MINE!

You use your work computer to check your personal social media accounts.

You click on an advertisement that installs malware on your computer.

MINE!

You attend a conference and receive a free flash drive as one of your souvenirs.

As soon as you plug it into your work computer, spyware is installed.

MINE!

You receive an email asking you to reset your password. You click on the link and enter your current password as well as your new one.

The email was a scam. You've just given hackers your login credentials.

MINE!

Your company uses an open wireless network.

A hacker who is near your building is able to get into your main corporate system through the wifi.

MINE!

You find a free version of a software program that your company needs, and to cut costs, opt for the free version rather than the commercial version.

When you download this version instead, you also download some harmful viruses.

MINE!

You receive an email from a government agency that states your organization is out of compliance with current regulations. You click on the link.

The email was spoofed! By clicking on the link, you download malware to your computer.

MINE!

Your social media profiles have information about your birthday, habits, family, and more.

A hacker is able to successfully impersonate you and answer all the standard security questions to “reset your password.”

MINE!

You receive an email from a credit card company that offers much better rates than your standard company cards have. You sign up without researching the company.

You've just given hackers important information about you and your business.

MINE!

A woman enters your office, claiming to be from the IT department. She asks you to log in to your corporate account so that she can fix a bug on your computer. You move out of the way so that she can do her work.

She then installs malware that infects the entire network and releases sensitive data.

MINE!

A job applicant is sitting nervously in the waiting room. She asks you if you would please make a copy of her resume for her. You agree, leaving your own computer unattended.

In the few seconds that your attention is elsewhere, she installs spyware on your computer.

MINE!

You find a USB drive in the parking lot outside your office. Wanting to return it to its rightful owner, you plug it into your computer and open a file.

You've just downloaded malware that will give the attacker access to your entire network.

MINE!

You receive an email from your work credit card company, informing you of a possible fraudulent charge. You click on the link in the email to investigate what the charge might be.

There are no fraudulent charges—instead, you just downloaded a Trojan into your company's network.

MINE!

While hanging out with friends one day, you begin discussing how you remember all of your passwords. You don't want to reveal your password but you say that you use your dog's name for all of your passwords.

But your friends know your dog's name, and they now can log into your accounts—both personal AND professional

MINE!

Your company allows you to use your own computer for work purposes. However, it does not check in on your security software and software updates.

You choose a cheap antivirus software, but it cannot protect against everything ... this leaves your entire company network vulnerable because of your computer!

MINE!

You receive a call from an IT service person who directs you through a series of steps that you need to do to update your antivirus protection.

The caller is not legit! Instead, she guides you through the process of disabling the antivirus program and instead installing malware.

MINE!

You share your password to an online site in order to give a consultant access.

However, you use the same password for all of your accounts, and she now can hack into any of these accounts using these same login credentials.

MINE!

You receive multiple invoices through email, which request payment for ads that you don't remember ordering. The invoices become increasingly urgent, stating that your payment is past due. You pay via credit card so that you remain in good standing.

However, the invoices are not real, and you just gave your credit card information to a scammer.

MINE!

You receive an email from your work credit card company, informing you of a possible fraudulent charge. You click on the link in the email to investigate what the charge might be.

There are no fraudulent charges—instead, you just downloaded a Trojan into your company's network!

MINE!

You do not update any of your network access codes and passwords after firing an employee.

She is angry and decides to hack into your system as payback.