



LESSON PLAN

Level:	Grades 5-6/7-8
About the Author:	Matthew Johnson, Director of Education, MediaSmarts
Duration:	5-6: 1 hour 7-8: 2-3 hours

Winning the Cyber Security Game

Table of Contents

Table of Contents

Overview	2
Learning Outcomes	2
Preparation	2
Procedure	3
Online Risks	3
Winning the Cyber Security Game	4
Designing a Cyber Security Game	5
Game Evaluation Rubric	6

Handouts

Cyber Security Tip Sheet
Cyber Security Game Instructions
Cyber Security Game Scenarios (Teachers' Version)
Scenario Cards
Risk Cards
Tool Cards
What is a Board Game? (Grades 7-8)
Analysing a Board Game (Grades 7-8)
Board Game Design Worksheet (Grades 7-8)

This lesson has been developed with the support
of CIRA, the Canadian Internet Registration Authority.





LESSON PLAN

Level:	Grades 5-6/7-8
About the Author:	Matthew Johnson, Director of Education, MediaSmarts
Duration:	5-6: 1 hour 7-8: 2-3 hours

Winning the Cyber Security Game

Overview

In this lesson students discuss their online experiences and learn how to minimize the potential risks that may be associated with them. Using the *Cyber Security Tip Sheet*, students explore the many tools and strategies that can be used to mitigate or prevent negative online experiences. Once they have reviewed these strategies and resources, students will extend and test their knowledge by playing a game in which they compete against other students to match a series of technological “Tools” to the “Risks” they can help to prevent.

Learning Outcomes

Students will display the ability to:

- recognize the potential security risks and drawbacks of engaging in various online activities
- use a variety of tools and techniques to secure and protect their online experiences
- apply principles of board game design through the creation of a Cyber Security game (Grade 7/8 only)

Preparation:

For all grades:

Photocopy the following student handouts:

- *Cyber Security Tip Sheet* handout
- *Cyber Security Game Instructions*

To prepare for the Cyber Security activity, teachers should:

- Read the *Cyber Security Game Scenarios (Teacher's Version)*
- Print **one** copy of the *Scenario* cards deck and cut out the cards
- Print **two** copies of the *Risk* cards deck and cut out the cards
- Print **three** copies of the *Tool* cards deck and cut out the cards

For Grades 7/8 only:

Photocopy the following handouts:

- *What is a Board Game?*
- *Board Game Analysis Worksheet*
- *Board Game Design Worksheet*

Procedure

Online Risks

Start the lesson by asking students about what they like to do online (*for example: playing games, going on social networks or virtual worlds, watching videos, etc.*). Collect responses on the board, then draw a chart with three headings: *Talk, Shop and Play*. Explain that aside from school and work, these three headings cover most of what we do online. Take the responses previously collected and have students sort them under the three headings.

Next ask students if any of them have had negative experiences doing any of the things that have been mentioned. (*There's no need to ask for details, just find out if students have had what they would consider to be bad experiences.*) Ask if they're aware of any risks or things that might go wrong in any of those online activities. Have students elaborate on some of the possible things that can go wrong (*again, they don't need to talk about anything that's happened to them personally*). Make sure that the discussion includes not just well-publicized risks such as stranger contact but also things that might seem to be inconveniences or annoyances – having someone bother you in a game, for instance, or clicking on a link that led somewhere you didn't expect.

Distribute the *Cyber Security Tip Sheet* and review it with students, drawing connections to the previous class discussion about online experiences and risks. Now read students the following scenario:

You visit *Congo.com* to buy a book for your Dad's birthday. After leaving that site you go to *VidWow* to watch some skateboarding videos, play *World of Chivalry* for awhile and then check out the free games at the *Big Burger* site. The next time you go back to *Congo.com*, the first thing they show you is a collection of skateboarding videos, a *World of Chivalry* strategy guide and a book of *Big Burger* coupons. Not only this, but ads for all of these things start showing up on your *SpaceFace* page. How did they know that much about you?

Ask students to identify the type of risk that is being presented in this scenario: students will probably identify it fairly quickly as "Cookies". Go through the Tools section under "Cookies" in the *Cyber Security Tip Sheet* and discuss with students how each of the tools listed there will help prevent Cookies from tracking what you do online. (*Browser/antivirus updates can increase your ability to block cookies; clearing your browser cache removes cookies that have been installed; a site's privacy policy should tell you exactly what cookies the site will install and what they will do; private browsing tools let you visit sites without cookies being installed on your computer; and secure sites encrypt whatever data you give them, so cookies are less of a security risk.*)

Explain to students that they are now going to identify risks and apply tools and strategies to some different scenarios.



Winning the Cyber Security Game

Distribute the *Cyber Security Game Instructions* and tell students that they are going to play a game that will teach them about what can go wrong online and what tools are available to prevent bad things from happening or fix things when they go wrong.

Divide the class into no more than 10 groups of two to three students.

Give each group one **Scenario** card and distribute the **Risk** cards randomly, two per group. (If any **Risk** cards are left over, hold on to them until Step 3 below.)

Give groups time to play the game:

1. First, group members need to identify the risk found in their **Scenario**.
2. If they do not have the relevant **Risk** card, they must acquire it from the group that has it by trading cards they do have. They may need to acquire cards that group needs by trading with other groups first.
3. If you have **Risk cards** that you did not distribute, students may also trade with you. However, they do not get to choose one of your **Risk cards**, but rather draw randomly from the remaining cards.
4. Once they have the relevant **Risk card**, they must use the *Cyber Security Tip Sheet* to identify two Tools which can be used to prevent or mitigate that Risk.
5. Students then declare to you which Tools they will use to prevent or mitigate the Risk. Use the *Cyber Security Tip Sheet* to see if they have chosen correctly; if they have, let them draw two **Tool cards**. They must now acquire – either from the cards they drew or by trading with other groups – **Tool cards** matching the Tools they have chosen.
6. The first group to correctly identify the Risk in their Scenario, acquire that **Risk card**, correctly identify and declare two relevant Tools and acquire those **Tool cards** is the winner. If you wish you may have other groups to continue to play for second, third, fourth place and so on.
7. Groups share their identification of Risks and Tools with the class.

Note: This is intended to be a fast-paced and kinetic activity as students trade with one another to get the cards they need.

Example of play:

A group of three students receives a **Scenario card** and two **Risk cards**. The *Scenario* card reads "You were in a hurry to check your *SpaceFace* account this morning so you accidentally typed www.spacface.com. Instead of going to *SpaceFace*, you landed on a site that's advertising orthopedic shoes!"

The group correctly identifies the risk in the scenario as *Cybersquatting*, but the **Risk cards** they received were *Griefing* and *Malware*. The three members of the group canvass the other groups, looking for someone that has *Cybersquatting*; the group that has that card, however, does not need either *Griefing* or *Malware* but *Cookies*.

The three students again canvass the other groups and find that the group that has *Cookies* needs *Griefing*. They trade *Griefing* for *Cookies* and then *Cookies* for *Cybersquatting*.



The group now consults the *Cyber Security Tip Sheet* and identifies *Bookmarks* and *Content Filters* as tools that can be used to prevent cybersquatting.

Now the group presents their **Scenario card** to the teacher, correctly identifies the associated risk and presents the **Risk card**, and draws two **Tool cards**, *Strong Passwords* and *Content Filters*. The latter is one of the cards they need but they must also have *Bookmarks*, so the students again canvass the other groups, hoping to trade *Strong Passwords* for *Bookmarks*.

What luck! A group that has a *Bookmarks* card needs *Strong Passwords*. The group makes the trade and then brings their **Scenario card**, their **Risk card** and their *Bookmarks* and *Content Filters* cards to the teacher. Because they're the first group to correctly identify the risk in their **Scenario card**, identify the tools used to prevent that risk and get the right **Risk** and **Tools** cards, they win!

Designing a Cyber Security Game (Grades 7-8 only)

Ask students to list their favourite board games. Once they have named a few, distribute the handout *What is a Board Game?* and go through it with them. As a class, select a game familiar to as many students as possible and analyze it with the elements identified in the handout. For example, the game *Monopoly* might be analyzed as follows:

Goal: To be the wealthiest player

Way to win: Last man standing — when all the players but one have gone bankrupt, the remaining player is the winner.

Competition: Players are mostly competing against each other (to buy the most properties and to make each other go bankrupt). There are also obstacles that make the game harder, such as the *Go To Jail* square.

Chance: How far you move is determined randomly. There are also *Chance* and *Community Chest* cards that may give or take away money.

Pieces: Each player controls one piece. All pieces are the same in terms of game play. Pieces are only taken off the board when the player is out of the game.

Board: The board "represents" a city with different streets on it. It's a circuit (you go around and around forever.) It has many special spaces: Traps (*Go To Jail*), Bonuses (*Go*) and Random (*Chance* and *Community Chest*). Nearly all of the other squares are Forks, because you have to choose whether or not to buy a property when you land on it. Properties someone else has bought are Traps.

Now divide the class into 4-6 groups and distribute the handout *Board Game Analysis Worksheet*. Have each group analyze another popular board game, using the worksheet, and then share their analysis with the class.

Once the groups have shared their analysis, each group designs their own board game, using the handout *Designing a Cybersecurity Board Game*. The board game students create should be based on the content of the *Cybersecurity Tip Sheet* and should require a thorough understanding of the tip sheet to win. If you wish, you may have students build their games and give them an opportunity to play one another's games.



Game Evaluation Rubric

	Excellent	Good	Satisfactory	Needs Improvement
Knowledge/ Understanding	Game clearly demonstrated an awareness and understanding of the risks relating to online security and the strategies and tools to prevent such risks.	Game clearly demonstrated an awareness and understanding of most of the risks relating to online security and the strategies and tools to prevent such risks.	Game demonstrated an awareness and understanding of many of the risks relating to online security and the strategies and tools to prevent such risks.	Game did not demonstrate an awareness and understanding of the risks relating to online security and/or the appropriate strategies and tools to prevent such risks.
Playability of Game	The goals, objectives and rules for the game were clearly communicated and all players understood what they needed to do to win.	The goals, objectives and rules for the game were fairly clear and most players understood what they needed to do to win.	The goals, objectives and rules for the game were understood with additional explanation. Some players had difficulty playing.	Goals, objectives and rules for the game were not clearly communicated. Players had difficulty playing.
Design	Game effectively integrated many elements from the <i>Game Design Worksheet</i> .	Game effectively integrated some of the elements from the <i>Game Design Worksheet</i> .	A few of the elements from the <i>Game Design Worksheet</i> were integrated into the design of the game.	Not many elements from the <i>Game Design Worksheet</i> were integrated into the game design.
Creativity	The game reflected considerable thought, was highly creative and was interesting and fun to play.	The game reflected good effort in making it interesting and fun to play and incorporated creative elements.	Effort was made to make the game interesting and fun, but some of the things made it harder to understand/enjoy the game. There were a few creative elements.	Little thought was put into making the game interesting or fun. The design demonstrated a lack of creativity.
Polish (Optional)	Students used a variety of methods to make the game board and pieces visually appealing.	Contrasting colors and at least 1 original graphic were used to give the game visual appeal.	Contrasting colors and "borrowed" graphics were used to give the game visual appeal.	Little color or fewer than 3 graphics were included.



Cyber Security Tip Sheet

Most of what we do online falls into one of three categories: *Talk*, *Shop* and *Play*. There are risks associated with all these activities that we need to be aware of so we can take the necessary steps to protect ourselves and our computers. Below is a description of some of the risks that can be encountered online and the tools you can use to avoid them.

Risks

Cybersquatting: Scammers will sometimes register a Web address that looks like it belongs to a real business, or one that can easily be typed by accident when you are trying to type in the real business's Web address .

Tools: Bookmarks, Content filters

Cookies: These are small files that your Browser saves on your computer. They often include things like your login and password. Cookies can stay on your computer for months and may even record everywhere you go online.

Tools: Browser and antivirus updates, Clearing your browser cache, Privacy policies, Private browsing tools, Secure sites.

Data theft: Your financial and personal information can be very valuable in the wrong hands!

Tools: Bookmarks, Blocking other users, Browser and antivirus updates, Clearing your browser cache, Creating strong passwords, E-mail encryption, Firewalls, Privacy policies, Privacy settings, Private browsing tools, Reporting online crime, Secure sites.

Too much spending: The ability to buy real or virtual things instantly when you are online can make it easy to lose track of how much money you're spending.

Tools: Prepaid credit, Content filters

Griefing: Some people enjoy annoying other people on purpose and ruining experiences that should be fun.

Tools: Blocking other users, Contacting sites and ISPs, Content filters, Privacy settings, User/vendor rating systems

Identity spoofing: It's easy to pretend to be someone else online: there are lots of fake *Facebook* profiles and *Twitter* accounts that pretend to be from someone they're not.

Tools: Blocking other users, Browser and antivirus updates, E-mail encryption, Firewalls, Managing your reputation, Privacy policies, Privacy settings.

Identity theft: Scammers can steal your *online identity* by getting access to your credit card or bank information or to other information you use to prove who you are.

Tools: Bookmarks, Browser and antivirus updates, Clearing your browser cache, Firewalls, Privacy policies, Private browsing tools, Reporting online crime, Secure sites.

Malware: These programs — which may pretend to be something useful or install themselves by getting you to click a box — can hurt your computer or even take control of it. Teens are especially at risk from malware because it is often bundled with things they like to download like games and music.

Tools: Bookmarks, Browser and antivirus updates, Firewalls, Secure sites.



Online fraud: It's easy to be taken in by people online who promise more than they are going to deliver. You can see a complete list of online frauds at <https://www.recol.ca/fraudprevention.aspx>.

Tools: Bookmarks, Contacting sites and ISPs, Prepaid credit, Reporting online crime, Secure sites, User/vendor rating systems

Phishing scams: E-mails that try to get information from you by pretending to be from a bank or other business.

Tools: E-mail encryption, Reporting online crime.

Spyware: Is a special kind of malware that collects information from your computer. Some spyware can even record everything you type.

Tools: Bookmarks, Browser and antivirus updates, Firewalls, Secure sites.

Tools

Now that you know the risks, here is a description of the different tools that can help to make you more secure online.

Bookmarks: Most browsers let you set *Bookmarks* or *Favorites* so you can go straight to your favourite websites.

Blocking other users: Almost every kind of online communication lets you block other users from contacting you.

Browser and antivirus updates: Your Browser is your first line of defense against Malware, but you need to keep updating it. The same is true for free or commercial antivirus software.

Clearing your browser cache: The cache is where your Browser saves Cookies on your computer, so you should clear it often.

Contacting sites and ISPs: Bad behaviour that is not criminal can be reported to a site or to the ISP that hosts it.

Content filters: Browsers, ISPs, websites and special software all offer ways of filtering out unwanted content.

Creating strong passwords: Choose a password that is at least seven characters long and don't use words that can be connected to you, like your pet's name. Change some of the letters to numbers or punctuation marks and use a mix of upper- and lower-case letters. Then customize the password for each site by adding the first and last letters of the site. (*bananas* becomes *b@nAn2s* and then *fb@nAn2sk* as your *Facebook* password.)

E-mail encryption: E-mails can be intercepted and read. Encryption software and some e-mail services allow you to encrypt your e-mails so they remain private.

Firewalls: These block unauthorized access to your computer. Make sure yours is activated in your Control Panel.

Managing reputation: Do a search for your name to see what impression of you is on the Internet. If you find things that you don't like, try to get them taken down. You can also publish things that reflect how you want to be represented online. Consider registering your name as a Web address (www.yourname.ca).

Prepaid credit: Some banks and credit cards offer prepaid credit cards which only let you spend a set amount.



Privacy policies: Any site that collects information from you should have a *privacy policy*. This should be written in language that is easy to understand and should explain what will be done with any information you give them. A good privacy policy also tells you how to get your information deleted if you want to.

Privacy settings: Social networking sites such as *Facebook* have privacy settings that let you decide who can see what on your profile. The default settings that are automatically set up for you are often not the most secure, so make sure yours are set to show your content only to your friends.

Private browsing tools: Most browsers have a function that lets you surf without saving anything in your cache.

Reporting online crime: Online crime can only be stopped if it's reported. If you know about successful or attempted crime online, visit <http://www.recol.ca/> to report it.

Secure sites: Secure websites use methods like encryption to keep your data safe. Look for a Web address that starts with "https" and a padlock icon at the top or bottom right of your browser window (**not** the Web site itself.)




User/vendor rating systems: Some commercial sites allow users to rate vendors based on their experience with them. Look for a good rating and positive comments. As well, some online games and virtual worlds rate users based on other users' feedback. You can use these systems to help fight griefing.



Cyber Security Game Instructions

Your teacher is going to divide you into groups of two or three students to play a game that will test your knowledge of cyber security risks and the tools that can be used to manage them.

This game involves three sets of cards:

	<p>Scenario Cards</p> <p>Describe a situation relating to doing something online.</p>
	<p>Risk Cards</p> <p>Have the names of types of risks that you can come across when you do things online.</p>
	<p>Tool Cards</p> <p>Have the names of tools you can use to prevent online risks.</p>

Here's what you're going to do:

1. Your group gets one **Scenario card** and two **Risk cards**. The **Scenario card** tells you about something that could happen to you online, while the **Risk cards** list some of the online risks you've read about in the *Cyber Security Tip Sheet*.
2. After you have read your **Scenario** card, take a look at your *Cyber Security Tip Sheet* and identify which of the Risks listed there is the Risk that your **Scenario Card** represents.
3. If you already have the **Risk card** for that Risk you're in luck – you get to skip to step 5. If you don't, you are going to have to get the card you need from another group by trading one of your cards. (You may have to do some trading around with a couple of groups before you have the exact **Risk card** you need.)
4. If your teacher did not hand out all the **Risk cards**, you can also trade with your teacher. If you do, though, you don't get to pick which card you get: giving your teacher one of your **Risk cards** lets you draw one randomly from the stack of cards that weren't handed out.



5. Once you have the right **Risk card** that matches your **Scenario card**, use the *Cyber Security Tip Sheet* to figure out what Tools you need to manage that Risk. When you have this figured out, tell your teacher which Risk and Tools match your **Scenario card**. If you're right, your teacher will let you draw two **Tool cards** from the deck.
6. If the **Tool cards** do not match the Tools for the Risk that's in your **Scenario card**, you will need to trade with other groups until you have both of the **Tool cards** you need.
7. If your team is the first to get the **Risk** and **Tool cards** that match your **Scenario card**, you win!



Cyber Security Game Scenarios (Teacher's Version)

1. You were in a hurry to check your *SpaceFace* account this morning so you accidentally typed www.spacface.com. Instead of going to *SpaceFace*, you landed on a site that's advertising orthopedic shoes-
Risk: Cybersquatting
Tools: Bookmarks, Content filters
2. Yesterday you bought some new songs at *MyMusicMart* with your *PayNow* account. Today you found out that someone else used your *PayNow* account to buy more than a thousand dollars' worth of stuff.
Risk: Data theft
Tools: Bookmarks, Blocking other users, Browser and antivirus updates, Clearing browser cache, Creating strong passwords, E-mail encryption, Firewalls, Privacy policies, Privacy settings, Private browsing tools, Reporting online crime, Secure sites
3. You were shopping at *MyMusicMart* yesterday and heard so many cool songs that you had to buy them all. Now they say you owe them \$200!
Risk: Excessive Spending
Tools: Prepaid credit, Content filters
4. All of your friends have been playing *World of Chivalry* so you decided to give it a try. As soon as your character appeared, though, a high-level character killed you and took all your stuff. You tried to keep playing but the same guy killed you every time you respawned.
Risk: Griefing
Tools: Blocking other users, Contacting sites and ISPs, Content filters, Privacy settings, User/vendor rating systems
5. When you went to school today your best friend was really mad at you. It turned out that she thought you had left some really mean comments on her *SpaceFace* page — but you didn't write them.
Risk: Identity spoofing
Tools: Blocking other users, Browser and antivirus updates, E-mail encryption, Firewalls, Managing reputation, Privacy policies, Privacy settings.
6. Yesterday you got a credit card bill for \$500 dollars in the mail — but you don't have a credit card! Someone used your name, your address and other personal information about you to apply for a credit card in your name.
Risk: Identity theft
Tools: Bookmarks, Browser and antivirus updates, Clearing browser cache, Firewalls, Privacy policies, Private browsing tools, Reporting online crime, Secure sites.
7. For the last month your computer has been getting slower and slower, and yesterday it finally wouldn't work at all. You had your big brother look at it and he found out that it was infected with dozens of viruses.
Risk: Malware
Tools: Bookmarks, Browser and antivirus updates, Firewalls, Secure sites.



8. You bought a new skateboard online with your *PayNow* account but the board never came. You've sent e-mails to the person selling it but haven't heard anything.
Risk: Online Fraud
Tools: Bookmarks, Contacting sites and ISPs, Prepaid credit, Reporting online crime, Secure sites, User/vendor rating systems
9. You got an e-mail from *PayNow* saying that there was a problem with your account. After you e-mailed them your login information, someone used your *PayNow* account to buy all kinds of stuff.
Risk: Phishing scam
Tools: E-mail encryption, Reporting online crime.
10. Yesterday you tried to log into your *SpaceFace* account but found out that somebody had changed your password. Then you found out your password had been changed on all of your online accounts. Your big brother did a scan of your computer and found a program on it that was recording everything you typed, including your login information for all your accounts.
Risk: Spyware
Tools: Bookmarks, Browser and antivirus updates, Firewalls, Secure sites.



You were in a hurry to check your *SpaceFace* account this morning so you accidentally typed www.spacface.com. Instead of going to *SpaceFace*, you landed on a site that's advertising orthopedic shoes!

Yesterday you bought some new songs at *MyMusicMart* with your *PayNow* account. Today you found out that someone else used your *PayNow* account to buy more than a thousand dollars' worth of stuff.

You were shopping at *MyMusicMart* yesterday and heard so many cool songs that you had to buy them all. Now they say you owe them \$200!

All of your friends have been playing *World of Chivalry* so you decided to give it a try. As soon as your character appeared, though, a high-level character killed you and took all your stuff. You tried to keep playing but the same guy killed you every time you respawned.

When you went to school today your best friend was really mad at you. It turned out that she thought you had left some really mean comments on her *SpaceFace* page — but you didn't write them.

Yesterday you got a credit card bill for \$500 dollars in the mail — but you don't have a credit card! Someone used your name, your address and other personal information about you to apply for a credit card in your name.

For the last month your computer has been getting slower and slower, and yesterday it finally wouldn't work at all. You had your big brother look at it and he found out that it was infected with dozens of viruses.

You bought a new skateboard online with your *PayNow* account but the board never came. You've sent e-mails to the person selling it but haven't heard anything.

You got an e-mail from *PayNow* saying that there was a problem with your account. After you e-mailed them your login information, someone used your *PayNow* account to buy all kinds of stuff.

You tried to log into your *SpaceFace* account but somebody had changed your password. You found out your password had been changed on all your accounts. Your big brother did a scan and found a program on it that was recording everything you typed, including your logins for all your accounts.

SCENARIO CARD

SCENARIO CARD

SCENARIO CARD

SCENARIO CARD

SCENARIO CARD

SCENARIO CARD

SCENARIO CARD

SCENARIO CARD

SCENARIO CARD

SCENARIO CARD

CYBERSQUATTING

COOKIES

DATA THEFT

**EXCESSIVE
SPENDING**

GRIEFING

**IDENTITY
SPOOFING**

**IDENTITY
THEFT**

MALWARE

**ONLINE
FRAUD**

**PHISHING
SCAMS**

SPYWARE

RISK CARD

RISK CARD

RISK CARD

RISK CARD

RISK CARD

RISK CARD

RISK CARD

RISK CARD

RISK CARD

RISK CARD

RISK CARD

BOOKMARKS

**BLOCKING OTHER
USERS**

**BROWSER/
ANTIVIRUS
UPDATES**

**CLEARING
BROWSER CACHE**

CONTACTING ISPS

CONTENT FILTERS

**STRONG
PASSWORDS**

**E-MAIL
ENCRYPTION**

FIREWALLS

**MANAGING
REPUTATION**

**PREPAID
CREDIT**

**PRIVACY
POLICIES**

TOOL CARD

TOOL CARD

TOOL CARD

TOOL CARD

TOOL CARD

TOOL CARD

TOOL CARD

TOOL CARD

TOOL CARD

TOOL CARD

TOOL CARD

TOOL CARD

**PRIVACY
SETTINGS**

**PRIVATE
BROWSING TOOLS**

**REPORTING
ONLINE
CRIME**

**SECURE
SITES**

**USER/VENDOR
RATING
SYSTEMS**

BOOKMARKS

FIREWALLS

**SECURE
SITES**

**CLEARING
BROWSER CACHE**

**PRIVATE
BROWSING TOOLS**

**BLOCKING OTHER
USERS**

**BROWSER/
ANTIVIRUS
UPDATES**

TOOL CARD

TOOL CARD

TOOL CARD

TOOL CARD

TOOL CARD

TOOL CARD

TOOL CARD

TOOL CARD

TOOL CARD

TOOL CARD

TOOL CARD

TOOL CARD

What is a Board Game?

Board games have been around for a long time: the oldest one known is the ancient Egyptian game *Senet*, which people played more than 4000 years ago. Today there are hundreds of different kinds of board games, but they all have certain things in common. These common elements are what you will decide on when you design your game.

Once you have learned about the common elements of board games and analysed a familiar game, you will design your own board game which will test players on their understanding of the Risks and Tools described in the *Cyber Security Tip Sheet*.

A goal: To be a game, there has to be something that all of the players are trying to do or get. There are four common types of goals in board games:

The Race: Players are all trying to be the first to get to a certain place on the board.

Examples: *Candyland*, *Snakes and Ladders*

Collecting: Players are trying to collect something and get the most of it.

Examples: *Monopoly* (players collect both money and properties), *Trivial Pursuit* (players collect "wedges")

Defeating an enemy: Players are trying to win a battle against one or more other players.

Examples: *Checkers*, *Chess*

Building: Players are trying to build one or more things on the board.

Examples: *Othello* (building lines in your colour), *Scrabble* (building words)

A way to win: Once you have decided on the goal, you need to figure out exactly *how* players win. Here are some of the most common:

First past the post: The first to reach a particular point wins.

Examples: *Snakes and Ladders* (first to the top), *Trivial Pursuit* (first to collect six wedges and answer a question in the middle square)

Last man standing: When all but one of the players have been eliminated, the player who is left is the winner.

Examples: *Monopoly*, *Checkers*.

Finite resources: The game ends when all resources have been used up or it is impossible for any player to make another move. At this point whichever player is in the strongest position wins (usually but not always based on the number of points).

Examples: *Scrabble* (all tiles have been used or no more words can be built), *Chess* (because the king cannot be taken, a game of *Chess* ends either when the king cannot make a legal move or when both players admit that neither can win [a stalemate])

Time limit: The game ends when a certain amount of time (measured either in hours or turns) has passed. At this point whichever player is in the strongest position (usually but not always based on the number of points) wins.

Examples: *Monopoly* (the "short version")



Competition: To make a game fun, there have to be things that make it hard for you to win. Here are some common examples:

Obstacles: Things that take you further away from winning.

Examples: The ladders in *Snakes and Ladders*, Go To Jail in *Monopoly*.

Other players: In some games (*Candyland*, *Snakes and Ladders*) all players just play against the game, but in most there are ways to make it harder for other players to win as well.

Examples: *Checkers*, *Chess* (capturing another player's piece), *Parcheesi* (sending another player's piece back to start), *Monopoly* (buying properties and charging other players rent when they land on them)

Chance: Except for pure strategy games like *Chess* and *Checkers*, most games have *random* elements that affect how the game goes. (Some games have several of these elements.) There are lots of different ways of adding chance to a game: with dice, with a spinner, drawing cards from a deck, pulling cards or tiles from a bag, flipping a coin, etc. Some things that may be affected by chance:

Moving: Chance decides how far your piece or pieces move.

Examples: *Snakes and Ladders*, *Parcheesi*, *Monopoly*. In *Trivial Pursuit*, the dice decide how far your piece moves but you decide in which direction it goes.

Fighting: Chance affects who wins in a fight between two pieces. Sometimes the result is *pure chance* (whoever rolls higher wins), but more often chance only *affects* the result.

Examples: *Risk* (each player rolls one die for each army in the fight and adds up all the dice; the player with the higher total number wins. Usually that's the player with more armies, but not always.)

Resources: Chance may determine what resources each player gets. This can happen at the beginning of the game, as the game goes on, or both.

Examples: *Monopoly* (you get random Chance and Community Chest cards when you land on those spaces), *Scrabble* (you get a random selection of letters at the beginning of the game, and at the end of each turn)

Pieces: In board games you control one or more pieces on the board.

Number: In some games you control more than one piece, in others just one.

Examples: *Monopoly* (one piece), *Parcheesi* (six pieces), *Checkers* (eight pieces)

Type: In some games all pieces are the same, in others pieces are different in some way that affects the play of the game.

Examples: *Snakes and Ladders* (all pieces the same), *Chess* (different kinds of pieces that each move differently)

Permanence: In some games pieces can be removed from the board, in others they cannot. In some games pieces can also be changed, either by the player or her opponents.

Examples: *Chess* (pieces can be removed from the board), *Monopoly* (pieces cannot be removed from the board), *Checkers* (pieces can move backwards and forwards once they reach the far side of the board), *Othello* (players can make the other player's pieces change colour), *Scrabble* (players can use other players' words to make their own)



Board: Finally, each board game has a board where the action happens. Sometimes a board is made to look like something in particular (a house in *Clue*, Atlantic City in *Monopoly*) but it can also just be plain squares (as in *Checkers* or *Chess*.) There are two important decisions to make about the board: its *shape* and whether or not it has *special spaces*.

Shape: There are four basic types of board game shapes:

Line: The board is a line from beginning to end. This is most common in race games.

Examples: *Candyland, Snakes and Ladders*

Circuit: Players go around the board in a loop.

Examples: *Monopoly, Trivial Pursuit*

Grid: The board is an equal number of vertical (up-down) and horizontal (left-right) squares. This is most common in strategy and building games.

Examples: *Checkers, Chess* (strategy games); *Scrabble, Othello* (building games)

Map: The board is divided into different "territories"; the map tells you how you can move from one territory to another.

Examples: *Clue, Risk*.

Special spaces: Many boards have spaces that are different from regular spaces, though some (for examples *Checkers* and *Chess*) do not. There are five common types of special spaces:

Traps: Landing on these spaces makes something bad happen, such as losing a turn, moving backwards or giving up a resource.

Examples: The Snakes in *Snakes and Ladders*, Go To Jail in *Monopoly*.

Shortcuts: Landing on these spaces moves you ahead or lets you jump over an obstacle.

Examples: The Ladders in *Snakes and Ladders*, the secret passages in *Clue*.

Bonuses: These spaces give you something that helps you in the game.

Examples: Roll Again in *Trivial Pursuit*, Double/Triple score spaces in *Scrabble*.

Random: Landing on these spaces may make something good or bad happen.

Examples: Chance and Community Chest in *Monopoly*.

Forks: Landing on these spaces gives you a choice about where to go or what to do.

Examples: Properties, Utilities and Railroads in *Monopoly* (buy them or not?), "spoke-ends" in *Trivial Pursuit* (go up the spoke or along the wheel?). Games with Map and Line boards often have spaces where you get to choose between one path and another.



Analysing a Board Game

Think about a board game that you like to play.

Name of game:

1. What is the goal of the game?

2. How do you win?

3. Competition: what do you compete against in order to win?

4. Does chance play a role in this game (for example, do you pick up random cards that make it easier or harder to get ahead?)

5. Are any pieces used in the game? Is everyone piece equal, or are some higher levels than others?



6. What does the playing board look like? Does it have a special shape?

7. Are there any special spaces on the board that give you an advantage or a disadvantage?



Board Game Design Worksheet

Using your knowledge of board game design, create a board game using the Risks and Tools in the *Cyber Security Tip Sheet*. Make sure that knowing and understanding the Risks and Tools are an advantage in playing the game (in fact, it should not be possible to win the game without understanding them.)

Design your board game by making the following choices. For each one, consider how you can make the Risks and Tools part of the game. Once you have finished designing your game you can create the board (either by hand or on a computer) and get whatever other items you need to use as pieces, random elements, cards, tokens, etc. Finally, write out the rules to your game in full sentences so that other people can play it.

1. What is the goal of your game?
How do the Risks and Tools relate to this?

2. How many players does your game have?

3. How do you win?
How do the Risks and Tools relate to this?

4. Do players compete against the game, against each other, or both? How?
How do the Risks and Tools relate to this?

5. What role does chance play in the game?
How do the Risks and Tools relate to this?



6. How many pieces does each player have?

7. Are there different types of pieces? If so, what are they?
How do the Risks and Tools relate to this?

8. What does your board look like?
How do the Risks and Tools relate to this?

9. What is the shape of your board?
How do the Risks and Tools relate to this?

10. What special spaces does your board have?
How do the Risks and Tools relate to this?

