Cybersecurity Awareness Month

Cybersecurity Awareness Month

Office of Information Technology / Division of Information Security

OCTOBER 2022

WEEK 1

CyberQwest

Grab a friend or three, roll the dice, and try to make it to square 64!

Clip out your game piece:

CyberQwest

Instructions

Number of Players
2-4

Age
6+

Components
Game board
Dice (2) (not included)

Game pieces:
- Laptop
- Computer Bug
- Mobile Phone
- Lock and Key

Object of the Game
Be the first player to reach the "YOUR DEVICE & INFORMATION ARE SECURED!" square #64.

Setup
Position the game board so all the players can easily move their pieces from square to square.

Everyone chooses a piece to play. Any extra pieces are out of play. Chosen pieces start off the board at square #1. Now get ready for the fun!

All about the squares:
Take a peek at the game board. The squares are numbered from 1 to 64. Players' pieces will move back and forth across the board, following the numbers upward - starting at square #1 and moving right toward square #8, then up to square #9 and left toward square #16, etc.

Of course, you can also move up by binary code ladders and sometimes go down, too, by sliding down crashed VPN tunnel chutes. More about that later.

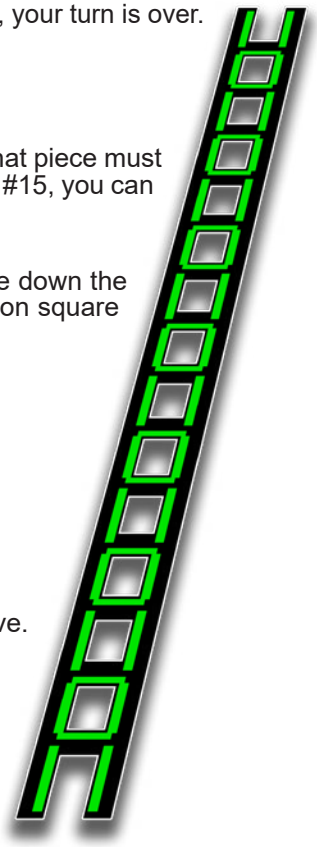
Game Play
Everyone rolls both dice. The player with the highest total goes first. Each piece begins the game on the "START" square #1. All turn taking proceeds to the left of the previous player.

What To Do On Your Turn
On your turn, roll the dice and move your piece, square by square, the total number shown on the dice. For example, on your first turn, if you roll a 5, move to square #6 on the board. Once you move your piece, your turn is over.
Note: Two or more pieces may be on the same space at the same time.

Going Up a Ladder Or Down a Chute

Binary Code Ladders
Any time a piece ends its move on a picture square at the bottom of a Binary Code ladder, that piece must climb up to the square at the top of the ladder. For example, if you end your move on square #15, you can immediately move up to square #36.

Crashed VPN Tunnel Chutes
When a piece ends its move on a picture square at the top of a chute, that piece must slide down the chute to the picture square at the bottom of the chute. For example, if you end your move on square #44, you must immediately move down to square #20.



Ending Your Turn
If your piece ends its turn on any of the following spaces, your turn is over:
- a square with no action described
- a square that a ladder or chute just passes through
- a picture square at the top of a Binary Code Ladder
- a picture square at the bottom of a Crashed VPN Tunnel Chute

End of the Game
The first player to reach the "Winner" square #64 wins the game. You can get there 2 ways:
1. Land there by exact count. If your dice roll would take you past square #64, don't move. Try again on your next turn, or
2. Climb there by ending your move on Binary Code Ladder square #31.

Game Over
Thank you for playing CyberQwest! We hope you had fun!

Game Tips

Here are some tips you can transfer from the game to real-life behaviors that can help keep sensitive information safe:

Space #5: Enabled two-factor authentication

Two-factor authentication offers another layer of protection by requiring more information, or an action, that proves authorized use. For instance, if you use your password or a PIN to access the IHS VPN, you also have to use your PIV Card, phone, or a token to gain access. Do this so that even if someone finds out your password, they will not be able to access your accounts. For more information on two-factor authentication at IHS, contact the Division of Information Security at cybersecurity@ihs.gov.

Space #15 Used a strong password

Using a strong password makes it harder to guess and increases the security of your accounts. Using a combination of letters, numbers, capitalizations, and special characters without using dictionary words can frustrate an attacker enough that they will try to find another victim.

Space #23 Reported a suspicious email

Even if the email is not malicious, go ahead and report it. Better safe than sorry. To report a suspicious email or other incident, forward the email to the Cybersecurity Incident Response Team at incident@ihs.gov.

Space #31 Confirmed email authenticity

Verifying an email's origin can be the difference between reporting an incident and becoming a victim. If the email's request seems unlikely, strange, or even if you have a gut feeling, do not reply to the email. Use a verified method to contact the person outside of email channels to confirm that they sent the request. If you are still unsure, contact the Cybersecurity Incident Response Team at incident@ihs.gov.

Space #44 Clicked on a pop-up

While many pop-ups are alerts about required updates, it is possible to download malicious software just by clicking on one. Ignore unfamiliar or unexpected pop-ups, especially if they warn you to 'Click Now!' or face a terrible consequence.

Space #46 Requested software update from IT Support

If you are concerned that your software version is out of date, contacting IT Support to request an update is good cyber behavior! Software updates may take time, but they include better security protections and increased functionalities that can make it easier to do your job safely.

Space #50 Used old software version

Related to #46 above requesting a software update from IT Support, old software versions are less functional and less secure than the most recent version; they may also be unsupportable in case you need assistance with a problem. Using old software is a security risk with the potential to expose IHS information to unauthorized persons.

Space #55 Used your birthday in a password

Using any personal information in your password reduces the security of your login information. Avoid including the following in your passwords: birthdays, names, cities, and address information, even ZIP codes. Because passwords should be hard to guess but easy to remember, you can use information about yourself to create a password without using exact details. For instance, the password 'mM@h3CWrmbMs&ms' can translate in plain language to 'My mother Alice has three children who are my brother, my sister, and me.'

Space #57 Didn't check email sender

Inspect the email sender information every time to make sure the message is authentic and can be trusted. Most email clients allow recipients to view the sender's name and email address. If you want to confirm an email's origin, hover your cursor over the sender's name, taking care not to click. If the information looks unfamiliar or seems suspicious, report the email to the Cybersecurity Incident Response Team at incident@ihs.gov.

Space #63 Shared login information

While it may be convenient to let another person use your login information because theirs has been lost or forgotten, this behavior is a violation of the IHS Rules of Behavior and compromises all systems where you have access. It also makes you responsible for any actions performed under your login. Encourage your colleague to open a ticket with IT Support at itsupport@ihs.gov so they can get assistance with accessing the information and systems they need. If they continue to ask for your login information, report the behavior to the Cybersecurity Incident Response Team at incident@ihs.gov.

Questions, Comments, and Suggestions

For more information on how you can protect sensitive information at IHS, contact our cybersecurity team at cybersecurity@ihs.gov.