Introduction
In Cyber Threat Protector (CTP), the goal is to build your network as quickly as possible so you can gain more points than your opponent. While you are doing this, you have to remember to defend your network because your opponent is going to try and disrupt your systems while building their network. For every attack there is a defense. For every defense there is an attack to get around it. The player with the most complete set of security defenses will be the one who is able to protect their critical systems and emerge victorious.
Preparation

A. You will need to have paper and pencil, or some other way to keep track of scores.

B. A single Cyber Threat Protector deck is needed for two players.

Game Objectives

A. The first player to obtain 20 points at the end of a round is the winner. If both players reach 20 points at the end of a round, play continues until the tie is broken.

B. If players have no cards to draw from the deck, then they must shuffle the shared discard pile and use it as the new draw pile.

C. Points are calculated at the end of each round. The total score cannot go below zero (0) points.
CTD Card Types

Asset Cards
These are your primary cards to build your network. They represent the physical assets you would encounter in a business, organization, or at home. This is how you gain points.

Event Cards
These cards represent various forces that can happen to your network and not the player playing the card. These Event cards are the only cards removed immediately after being played, as signified by their color.
Defense Cards
These cards are used to protect your network just as you would at home or in an organization. Defenses must be kept up to date. Failure to do so could have significant consequences for your network. Defense cards will prevent different types of attacks from harming your systems.

Attack Cards
These cards represent the various evil forces that exist on the Internet today and not the player playing the card. Attack cards will reduce your opponent’s points. Note: Defense cards may protect against these attack cards; some Attack cards remove Defenses.
Cyber Threat Protector cards vary in the information displayed. Some cards will list the names of other cards that it can remove from play; others will block cards from being played and some will have unique effects. Make sure to read the Card Abilities! A description of information found on a typical playing card:

**Anatomy of a Card**

Card Name

Card Abilities

Point Value

Card Information

**Game Setup & Notes**

A. Shuffle the cards. Once the deck is shuffled, both players will decide who will be player one. Then both players draw five (5) cards.

B. After a player has taken their turn, they will discard remaining cards in their hand and draw five (5) new cards before their opponent plays any cards.

C. Asset Cards do not need to be in play in order to play Defense/Attack cards. Some cards require other cards to be in play before being played. Some cards can only be used when specific cards are not in play. Some cards will not be allowed to have multiple in play.
Step 1
Player One will review the cards in their hand and choose four (4) cards they want to play. This is the only time that up to four cards are played. Each round after this, both players can only select up to three (3) cards to play.

Step 2
Player One puts the IP Spoofing card into play. This counts towards the limit of four cards that can be played by Player One during their first turn.
Step 3
Player One puts an Anti-malware card into play. This is the second of four cards that they can play.

Step 4
Player One puts a Desktop Computer card into play. This is the last card that they can play. While player one had the option of playing up to four cards, the remaining two (2) cards in player one’s hand require the opponent to have cards on their field that can be attacked, so they cannot be played.
Step 5
Player One then ends their turn. They will now discard their last two cards into a new pile, face up, called the Discard pile. They proceed to draw five new cards from the draw pile, and their turn ends.

Step 6
It is now Player Two’s turn.
Step 7
Player Two may play up to three (3) cards in their hand. Player Two uses their Anti-malware Not Updated card and targets Player One’s Anti-malware defense card.

Step 8
Per the effect of the Anti-malware Not Updated card, Player One’s Anti-malware is discarded. The Anti-malware Not Updated card remains on the field.
Step 9
Player Two puts an I Love You Virus card into play (which was not usable when Player One had Anti-malware in play). This counts toward their three-card limit.

Step 10
Player Two puts a Hardware Failure into play. This is the last card they can play for this turn.
Step 11
Player One will remove one asset from their field. In this case, the asset being removed is the Desktop Computer, because of the Hardware Failure. Both cards, Desktop Computer and Hardware Failure, will be sent to the discard pile immediately. Gold Event cards are immediately removed after they are played.

Step 12
Player Two will now discard their remaining cards to the shared discard pile face up and draw a new set of five cards.
Step 13
The round has ended, and it is time to update the players’ scores. Asset cards enable the player to gain points; however, Attack cards remove points played by the opponent. Note: Score cannot go below zero points.

Step 14
The score at the end of the first round is: zero points for Player One; zero points for Player Two. Remember, even in a situation where the final score each round is a negative number, the score tallied will not go below zero.

Note: There are no Asset Cards in play to gain points, and only Attack Cards that remove one (1) point each.
End of a Round

A. A round consists of one turn for each player.

B. Each player will add the points gained from their asset cards in play and subtract the points from their opponent’s attack cards in play. The scores for this round will be added to each player’s total score. The total score, however, will not be allowed to go below 0 points.

C. In the images below, the active player would gain 1 Point from the Desktop Computer, 1 Point from the ISP Connection and 1 Point from the Laptop Computer.

D. Since the opponent played two attacks, those points will count against the points gained.

E. For this turn, the active player is awarded 1 Point. This score is then added to the player’s total score.

F. Add or subtract points gained or lost after each round, until a player reaches 20 points or higher.
Note to Security Professionals
In developing this game, we recognize that we have taken some liberties with how things actually work. We have attempted to keep true to the spirit of computer security, but for playability reasons have slightly modified how things might actually work in reality. We believe, however, that the game is close enough that individuals playing the game will be able to gain some understanding of basic computer security concepts.

About the CIAS (Gaming)
The Center for Infrastructure Assurance & Security (CIAS) at The University of Texas at San Antonio (UTSA) is committed to creating a culture of cybersecurity through educational gaming programs. The CIAS conducts research into effective ways to introduce students to cybersecurity principles.

The CIAS’ Cyber Threat Protector game is designed for students in grades 3-5 to introduce cybersecurity terminology and defense strategies. Other cyber-related games include the popular Cyber Threat Defender®: The Collectible Card Game, Project Cipher and Pyramid of Knowledge. For more information, visit CIAS.UTSA.edu.

We’d Love Your Support!
By sponsoring Cyber Threat Protector, you are helping elementary students nationwide learn the basics of cybersecurity in a fun and engaging game that will prepare them for their future in cybersecurity!

For more information, please visit CIASGaming.com.

Note to Security Professionals
In developing this game, we recognize that we have taken some liberties with how things actually work. We have attempted to keep true to the spirit of computer security, but for playability reasons have slightly modified how things might actually work in reality. We believe, however, that the game is close enough that individuals playing the game will be able to gain some understanding of basic computer security concepts.