Stop the hacker, a Security Awareness Game

==

==

Game Overview

Game Description
5 to 7 players per game
2 proctors per game

By playing ***Stop the hacker***, players show their knowledge of cybersecurity best practices where user behavior protects the organization. A hacker will try to exploit one of the six staff roles, and they must use best practices inherent in the organization to avoid being hacked! The game will re-iterate the impact of user behavior to protect the organization from cyber threats.

The expectation is that staff should win nearly every game.

Author Recommendations:
Everyone gets a giveaway (prize) for participating. The hacker does not get a special prize for a "Win", because we don't reward threat actors.
People in our organization liked the playing cards, consider backing the player cards with the appropriate guidance card as packages to be used as a giveaway or participation prize.

***Game Over* Conditions:**

- Staff "Win": 3 staff choose the correct *Guidance cards*. They did their part to stop the hacker!
  - Rule Variants:
    - If there are less than 6 staff playing the game, numbers are reduced to 2.
    - Proctors may decide to go through all staff exploits/rounds rather than end after three successful preventative actions.
- Hacker "Win": 2 staff members are exploited (didn't choose the right Guidance card)

Proctor Roles:
Two proctors are needed for each game. Proctors should be Cybersecurity or Risk experts.

1. Proctor #1 (***Primary Moderator***)
   a. Read the rules script. Hand out player assignment cards.
   b. Throughout the game, ***Primary Moderator*** Instructs the hacker to choose a staff member to exploit by handing them a *red Hacked tag*.
   c. Once chosen, instructs the staff member to approach ***the Trainer*** for help.
2. Proctor #2 plays the role of **the *Trainer*** and keeps the solution cards and the *green **SAFE** tags*.
   a. If the staff member protects themselves by choosing the correct Guidance card, ***the Trainer*** gives them a green ***SAFE*** tag for them to wear (secured by a lanyard, clip or pin) and collects their red ***HACKED!*** Tag that was handed to them during gameplay.
   b. If the employee chose the wrong Guidance card, instructs the player to return to their spot and put the red ***HACKED!*** tag until the game is finished.

Game Sequence

Setting

- Larger versions of each card (role) can be displayed on posterboards/easels throughout the game zone.
- Each game expected to last 7 – 10 minutes (inclusive of game setup).
- Player groups should have a minimum of 5 players, and a maximum of 7.
- Each player group is assigned two Proctors. The Proctors will assemble players in a circle with a gameplay surface (a small table, chair, or other flat surface) in the middle.

Proctor Responsibilities (Game Setup)

Proctor #1:

Proctor #1 plays the role of the game moderator. Start by explaining the rules to the game cohort using the game scrip below:

> Welcome to our "Stop the hacker" game, where *you* follow preventative policy controls and best practices to help protect our organization! I will hand you a card indicating if you are either a staff member or the big bad hacker. Staff members, your role is to protect yourself from being exploited by choosing the correct guidance card from the Trainer. Hacker, your job is to successfully exploit the staff. The game ends when **2** staff members are exploited by you, *OR* staff prevent an attack by the hacker **3** times.
> *Proctor:* ***Adjust this script if using any rule variants.***

1. Hold out the Player Cards **face down** for payers to select. Players do not get the choose their role.
   Important: The # of player cards for your game cohort = 1 hacker card + X number of employee cards.
   The Trainer Card is not handed out to anyone in the player cohort, that is always given to Proctor #2.
2. Give players a moment to read their own cards. Do not reveal to other players.
3. Ask the hacker (only) to identify themself.

Proctor #2

Proctor #2 plays the role of ***the Trainer*** and provides additional support to move the game along.

1. Provide the hacker with three *red **Hacked!** tags* at the start of each game.
2. During the game, ***the Trainer*** offers guidance (in the form of Guidance cards) to players. The guidance card is a solution to prevent the exploit behavior that each player holds.

Game *Run of Show*

1. Start the game once everyone has received their player assignments.
2. Proctor #1: Instruct the hacker to choose a staff member to exploit by handing them a *red **Hacked!** tag*.
3. Once chosen by the hacker, instruct the staff member to read their card aloud (each player card contains a common mistake that may lead to employees being hacked/exposed)
4. Proctor #2: ***The Trainer*** will lay out all Guidance Cards on the play surface to help the staff protect themselves from being hacked. *The Trainer **DOES NOT** tell the players what their corresponding guidance card is.*
5. Staff member reviews the Guidance cards in a given time limit, and selects the correct user behavior for their player role:
   a. If the player chooses correct guidance to address their behavior, ***the Trainer*** will:
      i. Retrieve the "***Hacked!***" tag from the player and give them a "***SAFE***" tag.
      ii. Proctors ***may*** comment further on the best practices on the guidance card to educate all players.
   b. If the player chooses incorrect guidance:
      6. Player has been exploited! They keep and display the "***Hacked!***" tag for the remainder of the game.
      7. Hacker has achieved one point towards their win condition (2 points needed for hacker victory).
6. Repeat as necessary until the Game Over conditions are met (see Game Overview).

— END OF GAME—

Game Cards and Solutions

Player Cards

The Unintentional Insider

You left your security token in the office and plugged into your laptop overnight. An insider was able to crack your PIN and login to your account, now all your files have been breached, and your device is in quarantine until further notice so the cybersecurity team can perform forensics and clean the PC. Your PC will probably need to be reformatted.

The Unintentional Insider

You disposed of a classified document in the garbage can and it fell into the wrong hands. Now the colleague firm whose information was contained in the document needs to be contacted, general counsel is involved, and an investigation has been opened with the forensics team.

The Clicker

You clicked on a link or attachment in a phishing email, malicious code was downloaded onto your pc and a hacker gained access to all your data.

The Tea-Spiller

You overshared Company classified information on your Social Media platforms, giving hackers information on our systems and the architecture we use.
Now, if a vulnerability on our technology shows up, threat actors know we are using it, potentially before we can remediate the vulnerability.

The Carefree Traveler

You took your Company issued mobile device to an international destination without submitting your itinerary for review. Turns out you're in a restricted country, and due to privacy concerns, our devices are not permitted to be used there.

We suspect your data may be at risk for a compromise. An investigation has been opened, and the Vulnerability Management team will deactivate and swipe your device in the middle of your trip.

The Robot Friend

You used an Artificial Intelligence tool to help complete your work assignment.

Now our proprietary or confidential business intelligence is built into a multitude of Large Language Models and AI solutions.

Hacker Card

The Hacker

You are after the good stuff, Company data, credentials or application information that you can sell on the dark web or publish online to damage your reputation. Perhaps you'll lurk around our systems to see what we're doing that you can exploit or install a Ransomware kit on the Company network and use it to extort money.

A well-trained staffer is your kryptonite.

The Trainer card

The Trainer

We Prevent

We Detect

We work together to **Protect!**

Back of all cards:

Guidance Cards

Match for ***The Unintentional Insider (Token)***

Stop the hacker

GUIDANCE

Protect your security token!

- If you're working in the office, store it in a secure place apart from your computer, like a drawer or cabinet.
- Working remotely tomorrow? Transport the token separately from your laptop.

Match for ***The Unintentional Insider (Classified Document thrown in the trash)***

Stop the hacker

GUIDANCE

Do you really need to print it?

- Minimize printing whenever possible.
- If you must print, or you received printed information that is classified or sensitive, lock up or shred at the end of the day.

Solution for ***The Clicker***

Stop the hacker

GUIDANCE

Pause and think before you click!

- Interact with all unexpected, unfamiliar external senders with extreme caution.
- Never click on links or attachments until you have established trust.
- Try going directly to the link via an authenticated app or page you have bookmarked (Amazon, USPS, etc.)

Solution for ***The Tea Spiller***

Stop the hacker

GUIDANCE

Minimize your social media presence.

- You can say where you work, but don't talk about specific technology (versions) or project details.
- Don't take pictures at work.
- Don't let people or bots outside of our organization logon to your Company device to assist in deployment or troubleshooting.

Solution for ***The Carefree Traveler***

Stop the hacker

GUIDANCE

Based on the destination(s) on your itinerary, there may be an increased risk of espionage.

- Ask the Information Security team to review your itinerary at least10 business days in advance of your trip.
- Unless required, leave your Company-issued devices behind when you travel abroad.

Solution for ***The Robot Friend***

Stop the hacker

GUIDANCE

Just because you know an easier or faster solution exists, doesn't mean it's secure.

Complete work assignments only on approved platforms, software and devices issued by the Company.

A hacked player is issued this card to wear until the end of the game.

A player who selects the correct guidance card in allotted time gets to wear this tag until the end of the game

A separate file with all cards calibrated for printing can be provided on r equest, contact Sarae Winnicki

Photos from 2024 Events

Stop the Hacker