AWARENESS BATTLE GAME

Awareness Battle Game

In this game, players are divided into two teams: the Attackers and the Defenders. Each team is armed with a set of cards representing different cyber-attack scenarios and corresponding defense strategies.

The Goal

To outsmart your opponent and gain valuable insights into cybersecurity, all while having a blast!

Here's how to play:

Start: Gather friends and flip a coin to see who's an Attacker and who's a Defender. Each player gets 6 cards.

Play: Players take turns showing their cards. Attackers use their cards to try to breach defenses, while Defenders use theirs to stop attacks.

Adjust: After the first round, players can swap out one card for a new one to adapt their strategy.

Win: Play 6 rounds. The player with the most points at the end wins! Whether you're attacking or defending, it's all about learning while having fun.

AWARENESS BATTLE GAME

The table below can assist you in matching the appropriate attack and defense cards and determining the quantity of attack and defense cards needed.

Attack Cards	Defenses	Defense Cards
Malware	Use Antivirus/EDR	Use Antivirus/EDR
Phishing	1- Security Training 2- Secure Mail Gateway 3- dPhish	Use Antivirus/EDR
Ransomware	1- Backup	Multifactor Authentication
Dos and DDOS	1- Firewall Filtering 2- Network Redundancy	Secure Mail Gateway
Insider Threat	1- Access Control Policy 2- IAM 3- Monitor Data Access/usage	Use Antivirus/EDR
Man in the Middle Attack	Encryption	Network Redundancy
Zero Day	None	Access Control Policy
Social Engineering	1- Security Training 2- Multifactor Authentication	WAF
Brute Force	1- Multifactor Authentication 2- Password Policy 3- Lockout Policy	Encryption
Data Breach	1- DLP 2- Monitor Data Access/Usage 3- Access Control	Encryption
Physical Breach	1- Access Control 2- Security Training	Lockout Policy
Fileless Attack	1- Use Antivirus/EDR	Monitor Data Access/Usage
Vishing	1- Security Training	DLP
SIM Swapping	1- Multi-factor Auth 2- Security Training	IAM
Web Application Attacks	1- WAF	Monitor System resources
Identity Theft	1- IAM 2- Multi-Factor Auth	Restrict USB usage
Cryptojacking	1- Monitor System resources 2- Security Training	Hashing
USB Attacks	1- Security Training 2- WAF	Disbale autorun feature
Watering hole attack	1- Restrict USB usage 2- Disable autorun	Disbale autorun feature
Data Manipulation	1- Hashing 2- Encryption	Backups
Smishing	1- Security Training	
web Application Attacks		