Hackers

The security awareness game

Taktikal.

About the game

This game is a variant of the party game Mafia, also known as Werewolf.
In order for this game to serve its purpose to increase security awareness, we recommend using each attack as a learning opportunity. You can use the attack samples provided here or create your own.

About Taktikal

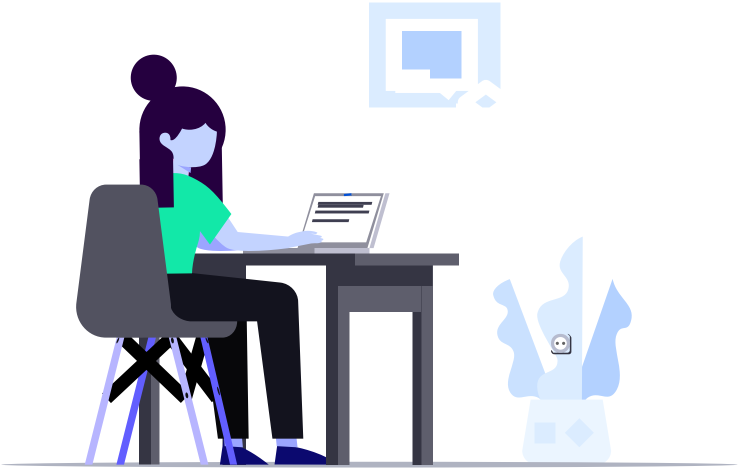
Taktikal provides an easy way for companies to collect signatures, digitize forms, and stay compliant with robust customizable workflows.
Taktikal developed this variant of the game to use for security awareness training within the company.

How to play

One person serves as moderator and steers the game while remaining impartial. The moderator hands out playing cards, describing each person’s role.

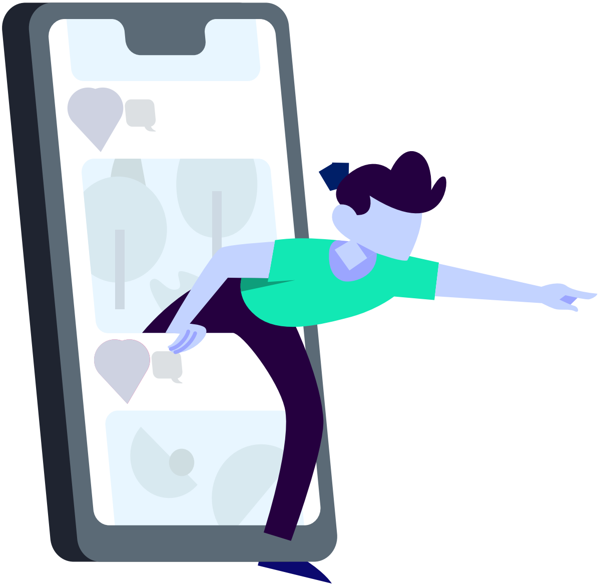
At “night”, all players close their eyes and the moderator calls on each role to wake up and perform their role with non-verbal methods before returning to “sleep”. Once all roles have been performed, the moderator wakes up the companies and reports on the attacks from the night.

During the “day”, the companies discuss who they think the hackers are and vote on who to eliminate each day.



COMPANY

The companies try to protect each other and find the hackers. They win if they can find all the hackers and eliminate them.



HACKER

The hackers work together and attack companies at night - their goal is to hack all the companies. During the day, they hide their identity.

SOC ANALYST

The SOC analyst tries to protect the companies. They can pick one person per night and find out if they’re a hacker. They win if the companies win.

HaaS PROVIDER

Each night the HaaS provider can check which company the hackers will attack that night. They can choose to save one company once during the game. They can also choose to attack a company once during the game. They win if the companies win.

Attack 1

This company’s CFO got a message on social media from a “friend” asking for their phone number and was then told that the friend had signed them up for an SMS-based game. If they received a code via SMS, they should forward that to their friend.

But the sender of those messages was, of course, a hacker. Once the hacker had the information on the phone number, they logged into the company’s online bank and sent an authentication request vis SMS. When the CFO gave them the code they were able to access all company funds and immediately started transferring money to offshore bank accounts.

Attack 2

An employee of this company received an email with a notice that they had been issued a traffic fine, which was attached to the email. Along with the fake notice, the employee downloaded a piece of malware that started logging all keyboard strokes and sent the information back to the hacker.

The hacker was able to use that information to log into their Google account, delete all backups, lock all employee access and encrypt the data using ransomware. The company paid $10 million in ransomware but the hackers still refused to return access to the data. The company never fully recovered from the breach.

Attack 3

An employee of this company took a meeting with a client at a coffee shop and then decided to stay and work a bit since it was such a nice atmosphere. They connected to the WiFi provided by the coffee shop and got to work. However, hackers had set up the WiFi, not the coffee shop, and they were able to spy on the employees traffic and steal usernames and passwords to various sites. The hackers then lurked in the companies systems for several months before publishing all their most sensitive data online. The company lost the trust of customers and went out of business.

Attack 4

This company’s CEO had an affair with a married woman. The woman’s husband happened to be a hacker, who discovered the infidelity and decided to take revenge.

The company had a critical project that the hacker knew about. The hackers conducted a DDoS attack using a botnet that was situated in various places around the world. The company needed to allow global traffic and did not have DDoS protection in place. They were unable to circumvent the attack. Since their site was down for 2 days during this critical project, their client sued for damages and the company was held liable and ultimately went bankrupt.

Attack 5

The hackers were monitoring a list of new vulnerabilites and on the day that a vulnerability in certain internet routers was announced, the hackers started scanning for unpatched vulnerable routers.

This company was not aware of the vulnerability and hadn’t patched their router in over a year. The hackers managed to infiltrate their router and access services which had been locked to outside access and deployed ransomware.

Attack 6

This company was visited by an electrician stating they needed to look at the wiring in the office. While doing so, the electrician (who was actually a hacker) saw information on employee computer screens regarding a sensitive law suit.

The hacker was able to sell the information to the company’s adversary causing the company to lose their law suit - which was critical to the company’s survival.