Who is the hacker

– game rules and instructions

Background:

The game is a role-playing game where participants take on roles as either law-abiding citizens or hackers. The objective for the law-abiding citizens is to report the hackers to the police before they themselves fall victim to hacking. Some players get a special role such as: PET*, IT consultant or IT-geek. Everyone hides their identity, because no one can trust hackers...

**PET is the national security and intelligence agency of Denmark*

The game is based on the well-known Werewolf concept, so several of the participants may be familiar with the concept already.

Only the game master needs to know the rules before the game begins. Making the game easy to get started with.

Throughout the game, players become aware of real-world cyber threats. They see examples on hackers' motivations, potential consequences, and how to recognize threats.

The game is designed for use in IT security training or as a professional team-building activity. No prior knowledge of IT or cybersecurity is required to play the game.

Preparation:

Number of players: 8-18. Time per game: 30-60 minutes depending on player count.

The playing cards needs to be printed out. The back of the cards should look the same, such that they cannot be distinguished from each other. There needs to be one card per player. See the distribution in Table 1.

The game master introduces the game and guides the game by explaining what is going to happen.

The players should sit around a table or in a circle. The game master should be able to move around the table, so they can get in proximity of everyone. Alternatively, players can stand in a circle with the game master in the middle.

Number of players	8	9	10	11	12	13	14	15	16	17	18
Hacker	2	2	2	2	3	3	3	4	4	4	5
IT geek	1	1	1	1	1	1	1	1	1	1	1
PET	1	1	1	1	1	1	1	1	1	1	1
IT consultant	1	1	1	1	1	1	1	1	1	1	1
Companies	3	4	5	6	6	7	8	8	9	10	10

How to play:

1. The introduction is read aloud by the game leader. See below.
2. The game master hands out a card for each player. It is important that the players keep their card secret.
3. The game master explains what happens in step 4-7:
4. Night phase
    a. Tell the players that it is night and that everyone must close their eyes and covers their face with their hands.
    b. Invite the hackers to wake up. Ask them to all point at a player they want to hack. Say that the PET agent is allowed to spy (open their eyes) while this is happening – but that they must be careful not to get exposed, so they will become the hackers' next victim. Then ask everyone to go back to sleep.
    c. Invite the IT-geek to wake up. Ask the geek to point to a participant of their choice. If it is a hacker, the game master gives a thumbs-up. The geek can thus over time find out who the hackers are. But, the geek must be careful not to call themselves out during the day phase. Otherwise he/she might end up as the victim next night. Tell the geek to go back to sleep.
5. Day phase
    a. Tell the players that night is over, and it has become day. Everyone can now open their eyes. The game master announces who got hacked. The victim shows their card to reveal their role. Read out the consequences of the hack (stated on the card). The victim is know excluded from the game. They can still watch, but are prohibited from interfering.
    b. Then invite the players to a discussion about who might be the hacker. After discussion; players must vote on who they want to report to the police. If it's a tie, no one will be handed over to the police.
    c. The player who is handed over to the police shows their card and reads the text on the card aloud.
    d. If the IT-consultant is hacked or handed over to the police, then he/she must select another player who will also be eliminated from the game.
6. It becomes night again – jump to step 4. Keep alternating between step 4 and 5 until either all hackers are caught by the police or all of the companies, the IT-geek, PET and the IT-consultant have been hacked.
7. The game master announces who has won.

Introduction

In a small country, hackers wreak havoc, turning cybersecurity into a national crisis. Local companies, intelligence agency PET, IT-geeks, and IT-consultants are scrambling to identify the perpetrators and report them to the authorities. Yet the task is daunting: trust is elusive, no one claims responsibility for the attacks, and the true identities of those involved remain shrouded in mystery.

The hackers strike under the cover of night, and each night another law-abiding citizen falls victim to their attacks. During the day, those that remain – both the law-abiding and the hackers – gather to discuss and vote out the suspected hackers. When night falls, the hackers return to their criminal activities. The game continues until all the hackers are caught, or all the law-abiding citizens have been hacked...

I will now hand out a card to each of you. On the card you can see which role you are to play. It is important that you keep your card secret.

Roles

- Hackers: Their goal is to hack as many as possible. Including: PET, geek and IT-consultant
- The IT-geek: Sometimes they know who the hacker is, but they don't dare to tell them directly, since it could make them victim.
- PET: Can spy on the hackers, but does it secretly
- IT-consultant: If the consultant is hacked or reported to the police, they bring another player with them in hope of catching a hacker.

Companies:

- Badminton Club
- Ministry of Defence Website
- The Hotel
- The Municipality
- The Bank
- Peter’s Facebook profile
- Sewage treatment plant
- Zealand Festival
- Great Belt Bridge (corporation that operates the bridge between Funen and Zealand)
- The webshop: Danish Photo Equipment

Law-abiding: Collective term for companies, PET, the IT-geek and the IT-consultant.

Follow-up in plenary

After the game, will be an obvious opportunity to discuss the following questions in the plenum:

- Have any of you experienced being hacked? Or know others who have?
- What are the consequences of hacking?
    - https://journalisten.dk/stort-mediehus-har-vaeret-udsat-for-omfattende-hackerangreb/ (translated)
    - https://www.dr.dk/nyheder/indland/stort-hackerangreb-mod-odense-universitetshospital-faar-omfattende-konsekvenser?_x_tr_hist=true (translated)
    - https://www.dr.dk/nyheder/indland/al-data-forsvundet-i-ransomware-angreb-chili-klaus-har-mistet-alt (translated)
    - https://nyheder.tv2.dk/krimi/2023-11-10-edc-er-blevet-hacket-knap-100000-cpr-numre-er-kompromitteret (translated)
    - https://nyheder.tv2.dk/samfund/2023-11-25-power-fik-628-millioner-forespoergsler-paa-40-sekunder (translated)
    - https://finans.dk/finans/ECE17054303/nordkoreansk-hackerangreb-har-lagt-dansk-virksomhed-ned/ (translated)

- https://www.tvmidtvest.dk/thisted/pro-russisk-hackerangreb-ramte-vestjysk-kommune-skal-vi-nu-ogsaa-traekkes-ind-i-det-her (translated)

HACKER

Cybercrime.

You hack to make money by extorting businesses. After you hack a company, you encrypt their data and demand a ransom.

HACKER

Cyberactivism.

You are a pro-Russian hacker group. You attack businesses to make their services unavailable. You are trying to change websites to show political propaganda.

HACKER

Cyberterrorism.

You work for a foreign power. Your attacks target critical infrastructure in order to destroy, for example, water and electricity supply, thereby terrorizing the civilian population.

HACKER

Cyber espionage.

You hack for a foreign power. You prefer to go unnoticed. You gather industrial secrets, state secrets, and the results of new research.

HACKER

Destructive cyberattacks.

You target networks and servers with the intent of disrupting infrastructure and control systems.

PET

You are employed by the Danish Police Intelligence Service. Your mission is to identify, prevent, investigate and counter threats to freedom, democracy and security in Danish society. You are a seasoned cyber threat intelligence analyst with expertise in covert monitoring of the dark web.

IT GEEK

You are an geek with a passion for exploring the world of technology. Occasionally, you come across evidence of hackers and, of course, report it to the authorities. However, you must tread carefully to avoid being mistaken for a hacker yourself.

IT CONSULTANT

You work for an IT company that offers server capacity for other companies. You know that anyone can be accused of being a hacker, but you have a plan. If someone accuses you of being a hacker, you will also shut down one of the customers you serve who you believe is a hacker.

THE BANK BANK

Consequences of hacking:

Hackers take down The Local Bank's online banking from 9:00 AM to 12:00 PM on March 31st.

THE GREAT BELT BRIDGE

Consequences of hacking:

When strong winds hit the Great Belt Bridge, barriers close automatically. On a calm July Saturday at 12:32, a hack triggers the wind gauge to show hurricane-force winds, halting traffic.

MINISTRY OF DEFENCE WEBSITE

Consequences of hacking:

A pro-Russian hacker group places a Russian flag on the front page of the Ministry of Defence website, and the site is very slow.

ZEALAND FESTIVAL

Consequences of hacking:

A hacker attack disrupts the ticket system on the festival's opening day, invalidating guests' tickets. Frustrated and impatient, they storm the festival grounds.

THE MUNICIPALITY

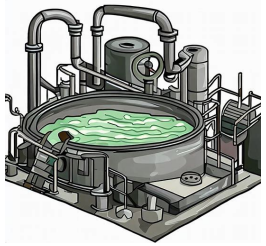
Consequences of hacking:

The municipality's housing benefit system is hacked, resulting in the deletion of all applications submitted over the past three months.

THE HOTEL

Consequences of hacking:

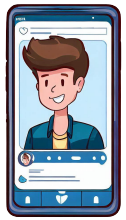
The hotel's booking system is hacked, and all bookings for the next two months disappear.



SEWAGE TREATMENT PLANT

Consequences of hacking:

A pumping system in the sewage treatment plant is hacked, which stops the pump and untreated wastewater flows into the nearby river.



PETERS FACEBOOKKONTO

Consequences of hacking:

Peter's Facebook profile has been hacked. He no longer has access to his Facebook account, and his friends are receiving spam from him on Messenger.

DANISH PHOTO EQUIPMENT - webshop

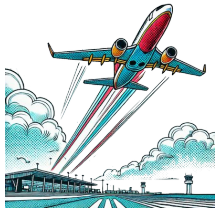
Consequences of hacking:

Hackers have taken over the company's data, which is now encrypted. The webshop has been told that the data will be released if they transfer 70,000 Euros to a specific account.

BADMINTON CLUB

Consequences of hacking:

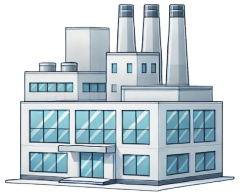
The chairman is looking for a backup of the most recent board minutes and the membership register is gone. The password for the website also doesn't work.



THE AIRPORT

Consequences of hacking:

A hacker attack on the airport's baggage system means thousands of suitcases are not sent on the correct flights, leaving travellers waiting for days for their luggage.



THE ROBOT FACTORY

Consequences of hacking:

Hackers break into a company's systems and steal confidential design files for a new product. Foreign competitors launch a copy before the company even reaches the market, leading to lost sales and weakened competitiveness.

THE HOSPITAL

Consequences of hacking:

A hacker cripples the hospital's IT system, preventing access to electronic medical records. Vital patient information is unavailable, and several surgeries have to be postponed, putting lives at risk.

ELECTRICAL GRID

Consequences of hacking:

Hackers infiltrate the power grid and cause a massive power outage across the city on a cold winter night. People are stuck in elevators, traffic lights are out, streets and shops are in darkness, and many households are also without water.