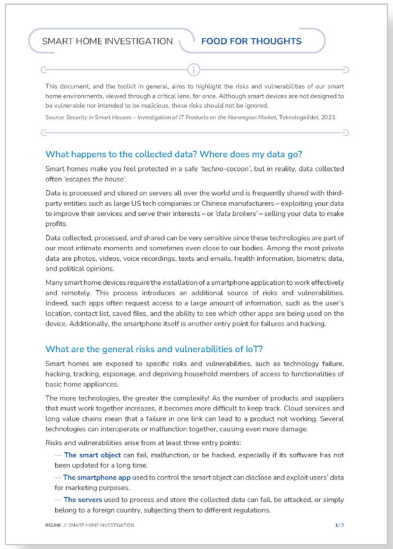
#3 MISSION DEBRIEFING

After you've explored your entire home, return to where you started and collect all the TECH CARDS.

Now, read the card sides providing information about sensitive data and risks. **Does it change your evaluation of these devices?**

Take a moment to read the '*Food for thought*' sheet to learn key issues at stake with regard to smart homes and IoT.



SMART HOME INVESTIGATION — FOOD FOR THOUGHTS

This document, and the toolkit in general, aims to highlight the risks and vulnerabilities of our smart home environments, viewed through a critical lens, for once. Although smart devices are not designed to be vulnerable nor intended to be malicious, these risks should not be ignored.

Source: *Security in Smart Houses – Investigation of IT Products on the Norwegian Market*, Teknologirådet, 2023.

What happens to the collected data? Where does my data go?

Smart homes make you feel protected in a safe 'techno-cocoon', but in reality, data collected often 'escapes the house'.

Data is processed and stored on servers all over the world and is frequently shared with third-party entities such as large US tech companies or Chinese manufacturers – exploiting your data to improve their services and serve their interests – or 'data brokers' – selling your data to make profits.

Data collected, processed, and shared can be very sensitive since these technologies are part of our most intimate moments and sometimes even close to our bodies. Among the most private data are photos, videos, voice recordings, texts and emails, health information, biometric data, and political opinions.

Many smart home devices require the installation of a smartphone application to work effectively and remotely. This process introduces an additional source of risks and vulnerabilities. Indeed, such apps often request access to a large amount of information, such as the user's location, contact list, saved files, and the ability to see which other apps are being used on the device. Additionally, the smartphone itself is another entry point for failures and hacking.

What are the general risks and vulnerabilities of IoT?

Smart homes are exposed to specific risks and vulnerabilities, such as technology failure, hacking, tracking, espionage, and depriving household members of access to functionalities of basic home appliances.

The more technologies, the greater the complexity! As the number of products and suppliers that must work together increases, it becomes more difficult to keep track. Cloud services and long value chains mean that a failure in one link can lead to a product not working. Several technologies can interoperate or malfunction together, causing even more damage.

Risks and vulnerabilities arise from at least three entry points:

- **The smart object** can fail, malfunction, or be hacked, especially if its software has not been updated for a long time.
- **The smartphone app** used to control the smart object can disclose and exploit users' data for marketing purposes.
- **The servers** used to process and store the collected data can fail, be attacked, or simply belong to a foreign country, subjecting them to different regulations.

RELINK // SMART HOME INVESTIGATION 1 / 3

But the biggest security risk with IoT devices is probably that we do not consider them as a risk. Users may not think twice about giving their name and address when setting up the device because it doesn't 'publish it' anywhere. But attackers can use these objects as gateways to penetrate more sensitive systems, a threat called 'lateral movement'.

For instance, attackers could use a smart thermostat to break into a family's network, using it as a backdoor to the devices it connects to. Thermostats don't usually have the same built-in protections as phones and computers, so they offer an easier route to do damage. For instance, a cyberattack on a smart thermostat might involve cranking up the heat in the house and lock it at this high temperature to extort a ransom.

Most common cybersecurity risks associated with smart products

- **Password Attacks** refer to situations where the attacker cracks the password of a computer system. Once the password is compromised, the attacker can gain unauthorised access to the system.
- **Malware** is malicious software designed to damage, disrupt, or gain unauthorised access to a computer system.
- **Denial of Service (DoS)** is an attack designed to disrupt the normal functioning of a computer system by flooding it with traffic, making it difficult for legitimate users to access the system.
- **Man-in-the-Middle (MITM)** is an attack where the attacker intercepts communication between two parties. The attacker can eavesdrop on the communication or alter the data being transmitted.
- **Social Engineering** is when the attacker tricks the user into revealing sensitive information. This information can be used to gain unauthorised access to the system, perform blackmail, or extortion.

What can be the harm and consequences for people and goods?

Smart homes have the particularity of putting household members at risk of being seriously harmed, both mentally and physically. On a larger scale, several smart homes malfunctioning together can disrupt key services and destabilise a part of society.

- **Goods and property** can be damaged; products that are supposed to protect the home's safety or ensure a stable ecosystem can lose function or be manipulated.
- **Information** can leak, be misused or exploited, either by criminals, foreign intelligence, or commercial companies.
- **Infrastructure (electrical, transport, etc.)** may be exposed. This applies in particular to power-demanding equipment such as electric vehicle chargers and hot water tanks.
- **People and welfare services** may be at risk: it can be a matter of life and death if equipment used for health and care loses access or changes function.

RELINK // SMART HOME INVESTIGATION 2 / 3

Well done, detectives!
Next, move to the SMART CRIMES investigation.

SMART HOME INVESTIGATION
OBSERVATION TOUR

A home tour exercise to view and review technologies of your everyday life

Smart home technologies are devices in the home that contain a computer and are connected to the Internet. They are often referred to as the '*Internet of Things*' (IoT).*

Internet of Things can be mistakenly perceived as a magical thing, operating without the need for back-end systems, infrastructure, impact, or human labour.

Additionally, smart objects are **designed to be so seamless in their use that we often '*forget*' about them**, especially in our domestic environments where they have become integral to our lifestyles.

The purpose of this exercise is to help you **(re)open your eyes to your familiar environment and recognise just how much technology and how many sensors are surround you – providing comfort, but also posing significant risks.**

**IoT, for 'Internet of Things', describes devices that embed sensors, connect and exchange data with other devices and systems over the Internet or other communications networks.*

In other words, they are items that contain a computer and are connected to the Internet, but are not used like a traditional PC, smartphone or tablet.

START YOUR INVESTIGATION >

#1 GET STARTED!

Alright detectives, let's practise some fieldwork!
For this activity, you need the following equipment:

The deck of TECH CARDS

A pen

A device can incorporate various technologies and multiple sensors, such as a camera, microphone, GPS, motion sensor, voice recognition, fingerprint scanner, blood pressure monitor, and more.

In this exercise, **we focus on identifying technologies and the sensors within each device to imagine what data can be collected**.

#2 SPOT THE SMART DEVICES

Let's start! Visit each room of your home and spot the technologies around. **Each time you spot smart tech or a sensor, pick up the matching TECH CARD**. For now, focus on the '*Evaluation*' side, without viewing the other side of the card (listing sensitive data and risks):

Take a moment to conduct your personal evaluation of this tech:

1. In your opinion, is it rather USELESS or USEFUL in your everyday life? In other words, is it closer to a gadget, or a key device?
2. In your opinion, is it rather INTRUSIVE or RESPECTFUL of your personal and intimate life? In other words, do you feel safe or spied on?
3. Does living with this technology in your everyday life make you feel rather VULNERABLE or IN CONTROL? In other words, do you master this technology, or do you feel mastered by it?

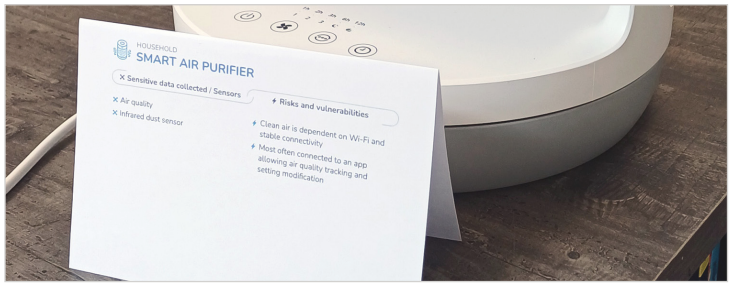
What you assess here is the '*smartness*' of the technology. Let's take the example of a smart fridge if you possess one: you assess the usefulness / intrusiveness / control of the smart dimension of the fridge, not a regular fridge.

Continue the tour until you have visited all the rooms.

TIPS

Did you check yourself as well?

Some *IoT* devices are wearable technologies: we carry them close to our bodies, often to achieve physical goals (e.g. fitness bracelets), health purposes (e.g. fall detection bracelets), or simply for convenience (e.g. smart watch).



You can **fold the card in half to make it stand upright and leave it where you spotted the technology**; this will provide a visual cue of how technologies are distributed throughout your home.

If you're doing this evaluation with your family, **grade these dimensions based on the average feeling of the group**.

HOW CAN YOU PROTECT YOUR HOME?

— **Disconnect from the cloud** by installing your own software on your smart home devices or opting for devices that can operate offline.

— **Review the data and privacy policies** of any downloaded apps, and use privacy tools like *Exodus Privacy* (exodus-privacy.eu.org) to analyse what data the app is collecting.

LEARN MORE ON SMART HOME SECURITY

Go to **nettvett.no** for further information and advice on protecting your smart home.

Congratulations, smart inspectors!

If you feel like it, replay your scenario to imagine a different (and happier) ending for the cases you solved:
What could have been done to avoid such a tragic issue?

Go on the OBSERVATION TOUR
if you haven't done so yet.

SMART HOME INVESTIGATION

SMART CRIMES

Build scenarios to imagine how a smart product driven crime case played out

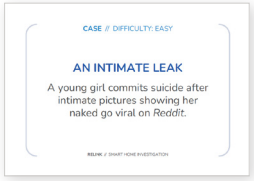
What could go (very) wrong with the smart objects we rely on in our everyday life? In this exercise, you will discover fictional cases inspired by true stories that highlight current issues related to the uses and misuses of the *Internet of Things*.

Your mission, should you choose to accept it, is to investigate (fictional) *'smart crime cases'*: you know the end of the story, but you need to understand how it happened and build up a sequence of events.

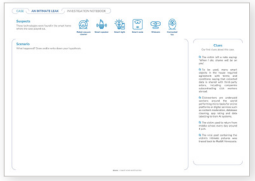
How did one or more smart objects (aka *'the criminals'*) fail or malfunction, leading to the tragic outcome? **There is no 'right' answer, but a variety of possible scenarios waiting to be imagined!**

#1 GET STARTED!

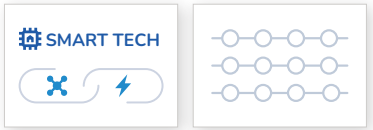
For this activity, you need the following equipment:



The deck of CASE CARDS



The INVESTIGATION BOARD



The deck of TECH CARDS

Sticky notes and pens

Pick up a CASE CARD and the INVESTIGATION BOARD that matches this crime case. Two difficulty levels are available; if this is your first investigation, start with one of the easier cases.

Check out the '*Suspects*' listed on the INVESTIGATION BOARD and display the matching TECH CARDS – fold the cards in half to make them stand upright around the board. You can also add the TECH CARDS matching the devices you previously spotted in your home.

#2 SOLVE THE CRIME

Take time to read the '***Clues***' section of the INVESTIGATION BOARD, as well as the sensitive data and risks associated with each TECH CARD.

Cross-reference this information to form your first hypothesis. Warning: In '*expert*' cases, some clues can be misleading!

Imagine the series of events that could lead, step by step, to the tragic outcome. Write and/or draw your favourite scenario on the INVESTIGATION BOARD.

SYNERGY CHALLENGE:

Imagine how several smart objects could be targeted or malfunction together! For an example, check the example case on the right.

EXAMPLE

THE CRIME CASE:

A family had to pay a ransom to a hacker to regain control of their smart home.

THE SCENARIO:

The smart printer software had not been updated for a very long time. Someone hacked it and gained access to the users' data. From there, the attacker infiltrated and infected the smart home's global security system. All the connected appliances in the house were blocked.

The users were then forced by the hacker to pay a ransom in cryptocurrency to regain control of their smart home.

#4 REFLECT ON YOUR FINDINGS

After the investigation, if you want to discover the true story that inspired the fictional case, check out the STORIES sheets.

There is no magic solution to protect yourself from IoT failures and attacks. Sometimes, the best smart home devices are the ones we choose not to buy!

If you're thinking of a clear-out, start by getting rid of the tech you found to be rather USELESS and/or INTRUSIVE. Why not dismantle the devices and recycle the components into low-tech mechanics, art pieces, or totems symbolising your newfound freedom?

If you are not ready to take the plunge, start by learning some basic tips to minimise the risks and vulnerabilities of your smart home:

— Assess the risks associated with the functions of each IoT and consider the possible consequences of equipment failure.

— Follow common Internet security practices: use strong passwords, enable two-factor authentication when possible, and keep software products up to date.