The interview was held in order to gain knowledge about what security risks a small business owner may face. As we want to develop an application that can help such users with improving their IT security, we saw that discussion how such a system may work with an IT specialist.

The informant has previously worked as head of IT Security and CEO of a small software company.

The informant tells us that the IT setup for small businesses varies based on the size and nature of the business. There are lots of different software products available that can fulfill the businesses’ needs.

Small businesses’ IT setups have more in common with larger businesses’ now than they did earlier. This is because more easily manageable software products are available to small businesses today. However, the business's IT setup depends on what service the company provides.

A hair salon only offers a service that takes place physically without IT systems. IT only supports the business in terms of bookings and handling money and customer data.

Whereas a software company has another kind of offering, more dependent on IT.

However, data protection is important to comply with any local regulations any business may have. Awareness is most important in general as this is the first step in creating internal processes and policies that describe how to navigate IT internally, and how the business will react if there is an attack.

The threats that a small business faces differ from those a larger business face. Attacks with malicious intent may not attack hair salons because their data isn’t as important. But phishing attacks are likely to happen to hair salon owners and employees, just as they happen to regular individuals as well. Therefore, having awareness training about concepts such as phishing and social engineering is really important, as most attacks are done through these methods and humans are the weakest part of a company’s IT security.

Our informant believes that customers usually look for a piece of software that can either advise on security or compliance, which is why these are separated. However, if a provider suddenly offers another branch of awareness in the existing software, then customers wouldn’t mind.

The informant tells us, that our app shouldn’t be intrusive, as we don’t want the business owners to think that this is a big undertaking that takes too much of their time to learn. A great idea to improve the app is to gamify it and give the business owners trophies for completing tests.

Lastly, the app shouldn’t share the statistics with employees in the company, as bad performance from an employee shouldn’t be laid out. Instead, the employees should want to talk about and brag that they have completed a new test successfully.