Comfort is important in identification

December 10 2015

VTT Technical Research Centre of Finland has conducted a study about user attitudes to different personal identification methods. The most popular identification methods were internet banking access codes and passwords. The most important thing to users seems to be the feeling of being in control of their own information and who else gets to access it.

Most of us have to deal with different authentication methods on a daily basis. We sign on to our computers and mobile devices; we authenticate ourselves when making credit card purchases or online payments - chances are, most of us are so used to many of the current methods of proving your identity or access rights that we don't have to think about them much.

"Convenience plays a large part also when using very traditional authentication methods such as passwords. In order to make remembering them easier, users resort using the same password in many places or choosing one that is easy to remember - which, incidentally, also makes it easy to guess," says researcher Katri Grenman.

In VTT's study, Italian and Finnish consumers were asked about their opinions of ten different authentication methods. The methods ranged from the very traditional (password, PIN code, internet banking access codes, mobile authentication, chip card reader, social media authentication) to biometric (facial recognition, fingerprint recognition and an RFID chip injected under your skin) and compared these with a new picture-based authentication method, where users selects points of interest in a photograph and proceeds to log in by touching the points in

a predetermined sequence.

Users were asked about their perceptions of the authentication methods' safety, convenience and the first impression regarding the lesser-known techniques. This was meant to gauge what kinds of things are important to people, how much weight they put on safety vs. convenience, and what needs to be communicated to users about the authentication methods they use.

Fingerprint recognition was popular both in Finland and Italy

Social media authentication is a topic that divides people into two quite opposing groups. On the one hand, many feel it's very convenient to access several services with one strong password you have memorised for your social media service of choice. On the other hand, there are the people who fear their information is being used for commercial purposes.

"Being used to something is important, when people decide what they want to use. Finns trust banks and are used to using their internet banking access codes for strong authentication. Bank access codes were at the top in our comparison", Grenman says.

Passwords also ranked among the most popular methods, and they are indeed almost impossible to avoid nowadays.

Fingerprint authentication was also among the top three authentication methods both in Finland and Italy. Its popularity is probably mostly due to convenience - it's impossible to forget your own identification at home or in the pocket of your other coat. Some users were worried about their fingerprint information leaking out, since you can't change

your fingers like you would a password. There were also fears of criminals cutting off fingers.

There are big differences between people in what they feel is important. For some, safety is paramount, and their attitude is reflected in the means they take to protect themselves. For others, convenience is the number one priority.

It's all very well telling people to use a different password for every service, but how realistic is that? If someone needs an account e.g. to access some content online, they might not feel that account information needs to be guarded like state secrets. Often, people have accounts that have limited of even fake information for unimportant services, and choose better and unique passwords for their more important accounts. If you bring the security thinking to the right level, it makes it easier for the user to commit to the security procedures and recognise what information really is valuable and needs to be protected carefully.

"The key factor for the users seems to be that they feel they are in control of their own information and who else can access it. It's usually a question of trust, and trust is slow to earn but quick to lose - often for good." Grenman says.

Provided by VTT Technical Research Centre of Finland