# Third-party access to bank accounts

**There are several third party providers offering intra-bank payment and account information services for e-banking customers. And although this may be convenient, there are some risks involved.**

**Protect yourself by...**

- not passing on your personal access data (password, PIN, ID number, etc.) for e-banking purposes to anyone - i.e. to no other person or any third party providers either.

To access customer bank accounts, they usually request and use their customers' e-banking access data. Passing on your personal access data to third parties however can lead to severe security risks for you as a customer. In addition, third parties can then transfer your bank customer data from Swiss financial institutions' very strongly regulated systems (FINMA, banking legislation, etc.) to environments which are less strictly controlled.

***Please be careful!***

*Both the use of impersonation and the non-regulated processing and storage of bank customer data harbour significant risks for you.*

***«eBanking - but secure!» therefore advises against passing any personal e-banking access data to third parties at all.***

## Further information for interested parties:

### High-risk use of intra-bank online services

Potential services by third party providers using customers' personal e-banking access data include such services as accessing bank accounts held with different financial institutions via just one platform. But watch out - by passing on your personal e-banking access data to any such platform, you are running severe security risks.

### Impersonation as a security risk

To access their customers' bank accounts, third party providers usually use a so-called impersonation facility (pretending to be or acting like someone else). To this end, they ask their customers for their personal access data (e.g. password and ID number) for their e-banking facility and then use these data to obtain unlimited access to these accounts in their role as an intermediary.

If you as a customer pass on your personal access data in this manner, this is similar to booking your holidays at a travel agency, then simply logging the person sitting opposite into your e-banking account and then leaving the shop - blindly trusting that this employee will now actually only debit the amount owed by you from your account, and will then log out again straight away. However, this person might as well just have a look how much salary you are paid every year, and might even be tempted to try and finance their own holidays from your account. Technically speaking, the use of impersonation is identical to identity theft - the same approach used in classical phishing attacks (https://www.ebas.ch/en/phishing/) - even if the third party provider is a respectable one!

With any inappropriate use of your personal access data, your bank will hardly be able to tell whether it is you as the customer yourself, a third party provider instructed by you or - in the worst case scenario - a criminal intermediary they are communicating with. This means the financial institution can no longer act with due diligence, for instance with regard to protecting their bank customer data to a sufficient extent. In the event of loss, you as a customer might even be threatened with liability exclusions.

### Loss of control over bank customer data

While Swiss financial institutions are subject to strict guidelines to protect their bank customer data and the security of their own systems, third party providers can save and process and store your data in environments which are much less well regulated if you give them your consent. These systems are partly neither owned nor controlled by such third party providers. This is because they often use so-called cloud solutions where the exact storage location of data is often unknown. And usually, Swiss client secrecy does not apply to such systems either!

The effects of this loss of control over the storage of personal data are incalculable. And if nothing else, this can make it easier for criminals to obtain access to personal bank customer data.