Security

Security at the e-commerce becomes more and more important. For example if you pay with your credit card you want to be sure, that nobody else except the seller, can get your payment information. To prevent the misuse of personal data for instance in the field of online banking and its transactions there are different TAN procedures.

TAN procedures

TAN is the shortcut for transaction number. In order to protect yourself from phishing attacks, one point is indispensable. The TAN and the e-commerce transaction must be on a different device. It is also important that the TAN can only be used for a defined space of time. The following three TAN-procedures provide the most secure standardization. At least one of those measures should be foreseen in a state of the art institute. (see: Authentication)

mobileTAN

During the mobileTAN procedure you get a sms (short message service) with the transaction number and the transaction information to your smartphone. As already noted above, for the highest protection, you should not receive the TAN and do the e-commerce transaction on the same device. So the mobileTAN procedure is not really mobile banking . A better name would be SMS-TAN. Just recently the mobileTAN procedure was discussed in public due to safety problems [http://www.checkpoint.com/press/2012/120512-media-alert-cp-versafe-eurograbber-attack.html](http://www.checkpoint.com/press/2012/120512-media-alert-cp-versafe-eurograbber-attack.html).

Sm@rt-TAN

If you want to use the Sm@rt-TAN procedure you have to buy a special card reader from your bank. This Sm@rt-device creates, together with your bank card and the input of the transaction information, a unique TAN, which is valid only a few minutes and only for this transaction.

Another method is the optical transfer of the transaction information. For example the TAN-device can read a black-white barcode on the monitor. The TAN-device convert them to the alphanumeric characters for startup code, account number and value of the transaction.

3D Secure

The “3D Secure” procedure was developed by Visa. Today it is known as the brandnames “Verified by Visa” and “Mastercade SecureCode”.

The intention behind is very easy. If a customer pays with the credit card at an online shop, he has to authenticate as the legal cardholder. Therefor he have to confirm the purchase with a self pre-defined password.
But not only at the payment, information will be sent through the internet. Even one step before. If you enter your private address and your shipping data, you also send a lot of private data through the internet. This data must also be protected. For this, there are several technical solutions. A must have for the internet shop provider are a **firewall** and an antivirus program.

**Firewall**

A **Firewall** should prevent attacks and spying from the internet as well as unauthorized access to the stored data.

**Antivirus Program**

An antivirus program scans the disk and the server for malicious programs. If the antivirus software finds such damage, it can be deleted, blocked or quarantined.

But also customers should have installed security software at their computers. In the internet there exists a lot of software against such programs. Here are some examples for freeware and software you have to pay for:

- [http://www.zonealarm.de/](http://www.zonealarm.de/)
- [http://www.avira.com/de/avira-free-antivirus](http://www.avira.com/de/avira-free-antivirus)
- [http://www.kaspersky.com/de/](http://www.kaspersky.com/de/)

But despite the numerous security software and security facilities it should be clear that a 100% safety can not be achieved. You should never blindly rely on such safety precautions and all ambiguities should be precisely checked.

— **Oliver Herrmann** 2012/12/03 13:27


From:
http://en.ecommercewiki.info/ - E-Commerce Wiki

Permanent link:
http://en.ecommercewiki.info/legal/security

Last update: 2012/12/12 18:36