Mobile payments and contactless payments

Payments via smartphone or contactless cards are becoming ever more popular. To shop with no need for cash or codes is convenient – yet it also involves risks.

This is how you pay cash- and contactless in a secure manner:

- Use the screen lock option to protect your mobile device against unauthorised access, and keep it up-to-date.
- Check which ones of your debit, credit and prepaid cards or mobile payment accounts you are actually using for your contactless payments. In case you don't use some of your contactless features, have them deactivated if feasible, and cancel or close any payment accounts you don't need.
- Specify limits for your cards or mobile payment accounts, and thereby limit the maximum risk involved, in accordance with your needs.
- Only load as much money onto your prepaid cards and payment accounts as you will need in the foreseeable future.
- Only ever actually divulge data to the mobile payment app, and only grant any such apps permissions which are absolutely necessary.
- Check your statements, and notify your provider immediately if you find any payments not carried out by you or which you don't recognise.
- Immediately notify your provider in case of theft or loss of your card or mobile device.

From the card in your purse to an app on your mobile device

It has long been possible to pay certain sums of money up to a certain amount by debit or credit card without having to enter a personal PIN code. For a number of years, it has now also been possible to use electronic processes such as Apple Pay or Twint to make contactless payments for your purchases via your smartphone or a smartwatch ("mobile payments").

Since the emergence of the Corona crisis, if not even before, we no longer seem able to do without these processes in our everyday consumer transactions. Mobile devices such as smartphones and tablets offer some obvious advantages: They are compact, almost always to hand and connected to the Internet.

In addition, mobile payment processes seem to become increasingly unavoidable: If you would like to install a chargeable app on your mobile app, you will have to enter your credit card details, and are then able to make "mobile" payments for online purchases, without needing your actual card to do so. Mobile payment options such as Apple Pay, Google Pay or Samsung Pay work in a similar manner – with the one difference that these can increasingly also be used for offline purchases, for instance at the supermarket or petrol station. The Swiss version Twint works in a similar manner, although you are not required to link this to a credit card, but can also do so to your bank account or a prepaid credit balance.

Copyright – All rights reserved. Lucerne School of Information Technologies

The risks of mobile and contactless methods

No matter how easy and convenient contactless payments are: Similar to your home computer, using your mobile devices and contactless cards every day entails certain risks and dangers. And it becomes easier to abuse these methods since there are no additional security elements such as a PIN code or password.

The following count amongst the most common risks:

- Physical loss or theft: In case your payment card or mobile device ends up in the wrong hands, there is a risk that they are used for unauthorised purchases. Depending on the payment method and spending limits, there is a risk of losing huge sums.
- Identity theft (https://www.ebas.ch/en/identity-theft/) : Fraud is also possible if you still have your card or device in your possession. By using some perfidious measures, such as the distribution of malware (https://www.ebas.ch/en/malware-infection/) , phishing messages (https://www.ebas.ch/en/phishing/) or social engineering (https://www.ebas.ch/en/social-engineering/) , attackers just might succeed in stealing your access and payment data in a purely digital manner, to then purchase items or order money transfers in your name.
- Privacy infringements: The app provider should not be able to find out what a customer has bought where. And retailers should not be able to establish what their customers' bank balance is. Whether this is actually the case is very difficult to check. Which of your data can be used in what way and by whom is eventually up to yourself.The good news: You can effectively protect yourself against all these negative scenarios by following our recommendations above.You can find detailed information on this topic in our "Mobile banking and Mobile payment" info sheet (https://www.ebas.ch/wp-content/uploads/2019/10/mobilebankingSKP_en.pdf) and in our article on Mobile banking (https://www.ebas.ch/mobilebanking) .

"Mobile payment" means cashless and contactless payments via mobile devices such as smartphones, smartwatches and tablets. Debit and credit cards also offer a contactless feature and are increasingly linked to mobile payment apps, too. To enjoy the convenience of these processes, you should take several precautions though to ensure your data and money are safe.

Copyright – All rights reserved. Lucerne School of Information Technologies