swisscom

Press release

Swisscom tightens security for customer information

Swisscom is to tighten security for so-called non-sensitive customer data in the wake of the misappropriation of a sales partner's access rights. Swisscom was unable to identify any activities against its customers as a result.

In autumn of 2017, unknown parties misappropriated the access rights of a sales partner, gaining unauthorised access to customers' name, address, telephone number and date of birth. Under data protection law this data is classed as "non-sensitive". Prompted by this incident, Swisscom has now also tightened security for this customer information. The data accessed included the first and last names, home addresses, dates of birth and telephone numbers of Swisscom customers; contact details which, for the most part, are in the public domain or available from list brokers.

Swisscom collects this customer information legally: It is required when entering into a subscription agreement. Sales partners are given limited access to this data to enable them to identify and advise customers and conclude or amend contracts with them. The system access required for this is protected by specific user logins and passwords. The contact details of around 800,000 Swisscom customers were affected by the breach – mainly mobile, and a few fixed network subscribers. Swisscom discovered the incident during a routine check of operational activities and made it the subject of an in-depth internal investigation.

Swisscom stresses that the system was not hacked and no sensitive data, such as passwords, conversation or payment data, was affected by the incident. Rigorous long-established security mechanisms are already in place in this case.

Tighter access control also for customer information; a stop on high-volume queries

Although the misappropriated personal data is classified as "non-sensitive" under data protection legislation, investigating the incident is a top priority for Swisscom. The relevant partner company access was blocked immediately. Swisscom also made a number of changes to better protect access to such non-sensitive personal data by third-party companies. These changes are summarised below:

- Access by partner companies will now be subject to tighter controls and any unusual activity will automatically trigger an alarm and block access.
- In the future, it will no longer be possible to run high-volume queries for all customer information in the systems.
- In addition, two-factor authentication will be introduced in 2018 for all data access required by sales partners.

These measures mean that there is no chance of such a breach happening again in the future. Swisscom has reported the incident to the Federal Data Protection and Information Commissioner (FDPIC). It is also considering legal proceedings and reserves the right to bring charges.

How can customers inform and protect themselves?

So far, Swisscom has not identified any rise in advertising calls or other activities against affected customers. There is no evidence of any harm to customers. In its commitment to transparency, Swisscom regards it as a priority to inform customers about the misuse of sales partner access rights and how to protect themselves from any possible misuse in the future. Towards this end, Swisscom is offering the following support:

- Mobile customers can send an SMS with the word "Info" to 444 to discover whether their name, phone number, address or date of birth were affected.
- Swisscom generally advises customers to be wary of any unusual or cold calls and recommends activating Callfiter for mobile and fixed network lines to block unsolicited cold calls.
- Customers are of course welcome to report any increase in calls from unknown numbers to Swisscom.

Berne, 7 February 2018

Swisscom.ch/News:

Interview with Philippe Vuilleumier, Head of Group Security – available from 10:00 a.m.