

Cyberattack on Compensation Office Swissmem – Information Letter for Employees of Affiliated Companies

Dear Sir or Madam,

We are writing to inform you about a security incident involving the Compensation Office Swissmem (CO Swissmem). As an employee of a company affiliated with the CO Swissmem, this communication is intended to keep you informed.

Despite robust security standards, the CO Swissmem became the target of a cyberattack—a criminal attempt to access the IT systems of organizations or companies to steal, delete, or encrypt stored data. Upon discovering the incident over the weekend of January 4-5, 2025, our specialists immediately isolated the systems from external access. After a brief outage, the fully rebuilt IT systems have been operating normally again since Thursday, January 9, 2025.

Comprehensive analysis and security measures were promptly initiated with the support of external specialists. The legally relevant authorities, including the Federal Data Protection and Information Commissioner (FDPIC), the Federal Social Insurance Office (FSIO), and the National Cyber Security Centre (NCSC), were informed and involved. Additionally, the CO Swissmem reported the attack to the Zurich Cantonal Police and filed a criminal complaint.

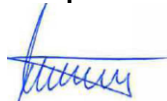
Our analysis to date has revealed that data from the CO Swissmem was encrypted and locked during the attack, but we successfully recovered all data. No attacks on bank accounts occurred, and no money was stolen.

Unfortunately, it has now been confirmed that data theft did occur. The stolen data may include various types of information, ranging from administrative data related to the CO Swissmem's operations to personal data, including information about benefits, contributions, or salary details. **At this time, it is unclear which specific data was affected, making it impossible to determine whether your personal data is involved.** To date, there is no evidence that the stolen data has been misused or published by the attackers.

Nonetheless, we advise you to exercise heightened caution: Be particularly vigilant about suspicious mail, emails, messages, or phone calls requesting personal information or encouraging unusual actions. Under no circumstances should you disclose personal data or banking details without thorough consideration. Specific recommendations are provided on the reverse side of this letter.

We deeply regret this incident and sincerely apologize for any inconvenience or issues it may cause. At present, we are unable to provide further details regarding the specific data affected.

Kind regards
Compensation Office Swissmem



Thomas Sommer
President



Damian Keller
Director

→ Please refer to the reverse side for important security and behavioral recommendations.

Security and Behavioral Recommendations

- Remain vigilant regarding suspicious mail, emails, messages, or phone calls that request personal information or encourage unusual actions.
- Do not click on links in unsolicited emails or SMS messages, particularly if they create a sense of urgency or threaten consequences.
- Do not allow yourself to be intimidated or pressured.
- Never disclose passwords or PINs via phone or email.
- Refrain from sharing personal information or bank account details without careful consideration.
- Do not grant access to your computer to unknown individuals, even if they appear trustworthy.
- Never hand over cash or other valuables to someone you do not know.

If in doubt, the National Cyber Security Centre (NCSC) is available to assist you with assessments and recommendations for further action: <https://www.report.ncsc.admin.ch/en/>.

If you are threatened, extorted, or suffer a loss, please report the case to your local cantonal police or, in emergencies, contact cckova@kapo.zh.ch, 112, or 117.