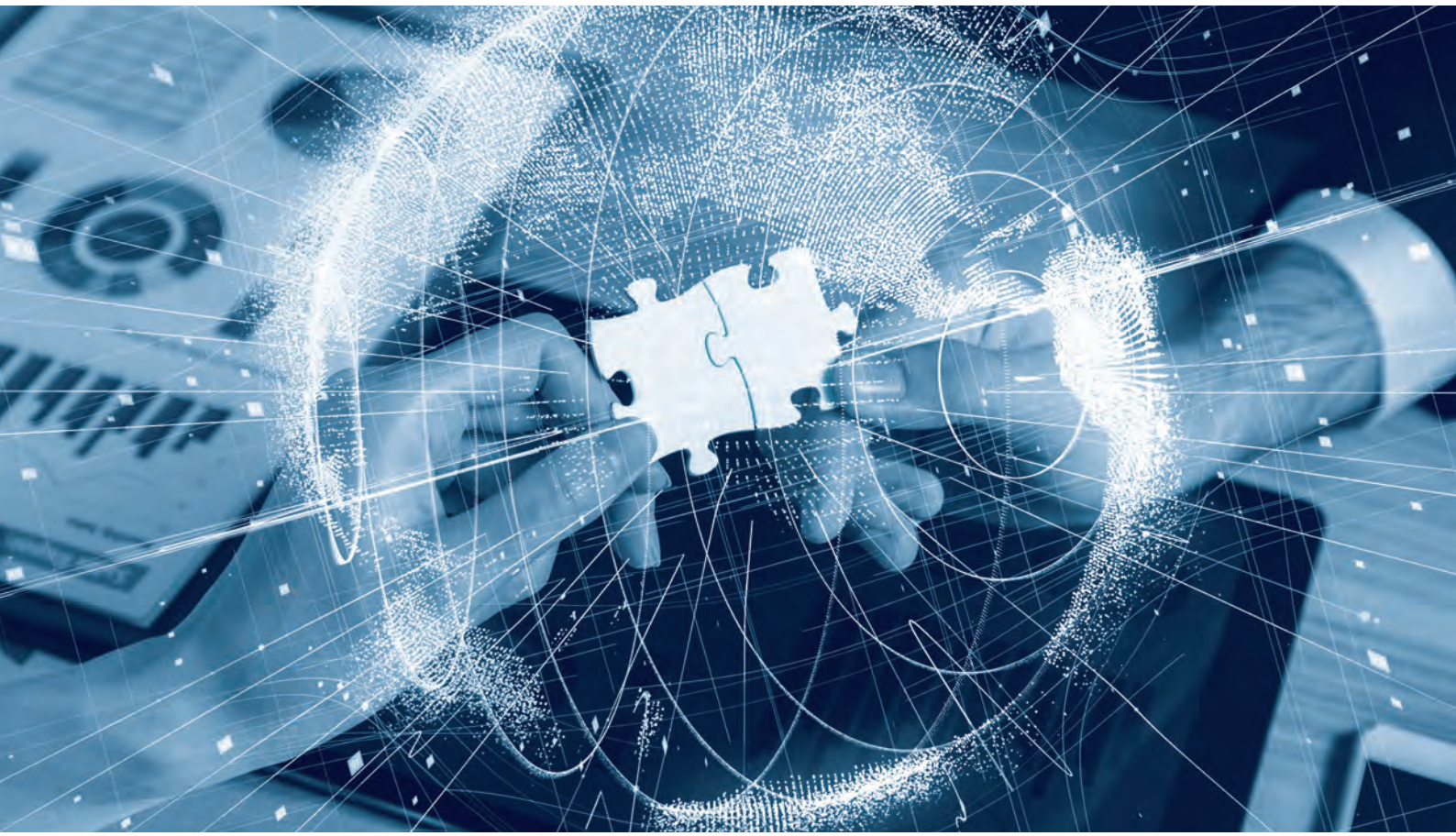
eCall
Business
Messaging

This is how eCall protects your data against hackers

Two-factor authentication



This is how eCall protects your data against hackers

eCall Business Messaging

They are deemed to be the greatest risk factor for IT security: passwords[1]. Again and again cybercriminals succeed in breaking into databases and cause great damage. eCall's two-factor authentication helps you to effectively protect your company's sensitive data.

1 https://www.searchsecurity.de/meinung/Passwoerter-Der-groesste-Risikofaktor-in-der-IT-Sicherheit

Companies invest a lot of money in the latest technologies to protect their IT infrastructure and data against unauthorised access. However, very often the technologies used are not the weakness but human beings themselves. More and more frequently attacks take place as a result of users' mistakes, for example, due to the selection of weak passwords or incorrect storage of passwords. No new ideas, or are there?

Humans, a security risk

Sound familiar? Post-it notes with passwords under the blotting pad or sometimes even attached, easily visible, to the display When selecting passwords one simply uses digit/word combinations that can easily be remembered. It's even worse than that: The same weak password is used for various online s ervices. Not a situation from the past, but the status quo This is demonstrated by top 10 most commonly used passwords in Germany as determined by the Hasso-Plattner-Institut (HPI) 12.9 million «.de» email addresses served as a data basis.

Undisputed winner in 2017: 123456

Rank	Password
1	123456
2	123456789
3	1234
4	12345
5	12345678
6	hallo
7	passwort
8	1234567
9	111111
10	Hallo123

Source: https://hpi.de/pressemitteilungen/2017/die-top-ten-deutscher-passwoerter.html

The domino effect and the resulting consequences can, in the event of an attack, cause significant damage.

Social Engineering – reaching deep into the bag of tricks

Even when passwords are handled professionally and responsibly, data and stealing of identities cannot be excluded. For this cybercriminals like to reach into the psychological «bag of tricks» and exploit users' weaknesses . With phishing mails, vishing calls (voice phishing) and other attacks employees are consciously manipulated or deceived with the goal that they «voluntarily» disclose sensitive data or passwords to the attacker. All these methods are consolidated under the term Social Engineering.

One click too many

The use of malware is another widespread method for getting to users' confidential access data. One click on a «malicious» link in an email is enough for a user to unconsciously install malicious software on a computer! Afterwards, for example, with a keylogger user's keyboard entries can be recorded and later be read out. According to a recent study by US scientists, in the meantime, a thermal imaging camera can even detect a password by using the heat traces. This is particularly easy to read out from users' entries made using the "two finger search system".

For this reason the increasing digitalisation and the new legal regulations, above all the EU data protection regulations (GDPR), require safe authentication methods to effectively protect company's, customer's and employee's data.

eCall
Business
Messaging

This is how eCall protects your data against hackers

More security with two-factor authentication

A common and proven method for protecting accesses and logins in the internet against unauthorised access is the two-factor authentication. Here an additional barrier against fraud is installed. In addition to the entry of a user name and a password, the user must identify himself using a further component in the form of a code or a token. Even if access data gets into the wrong hands, these additional authentication components can prevent online fraud attempts.

Sending access codes via SMS and voice messages to mobile phones

The Software-as-a-Service (SaaS) solution eCall helps you to make sure that the right information is available to the right person at the right time. By using mobile transaction numbers (mTAN) the authorised users can be given access codes via SMS or voice messages. This function gives you and your users better protection against data theft. For highly sensitive information the «High Privacy» option, where all contents are overwritten by the system after processing, is recommended. This option is especially suitable for sectors where highly sensitive data is managed, for example, finance & banking, health service but also insurances. Once the SMS has been sent a reconstruction is no longer possible.

Good reasons for a two-factor authentication via SMS

- Usernames and passwords are no longer secure enough
- The EU General Data Protection Regulation (GDPR) requires secure authentication options
- Today, virtually everyone has a mobile phone and can receive SMS messages. Therefore, eCall can be implemented as a cost-effective and simple SaaS solution with existing IT infrastructure
- Simple connection to interfaces (API) and to software from global providers such as RSA SecurID Appliance, SMS Passcode (via web service), and SafeNet (via HTTPS).
- Absolute reliability, high availability, and fast message transmission
- High dispatch quality at home and abroad through «SMS routing finder»
- Leading business messaging provider in Switzerland

See for yourself! Test it free of charge without any obligation via www.ecall.ch.

F24 – Your reliable partner for emergency notification, crisis management and critical corporation communications.

F24 is the leading software-as-a-service (SaaS) provider for emergency notification and crisis management FACT24) and for sensitive and critical communications (eCall) in Europe. With FACT24, F24 offers a highly innovative solution and helps customers all over the world to successfully and efficiently manage incidents, emergencies and critical situations. F24 AG is the first and only non-American provider listed in the latest Gartner Report for emergency/enterprise mass notification services (EMNS).

With its headquarters in Munich, Germany, the company is subject to German data protection laws and regulations and hosts its FACT24 SaaS system exclusively in German data centres. Furthermore, applying a variety of additional measures, F24 ensures added protection for both national and international FACT24 customers alike. Enterprises that select FACT24 are ideally prepared for any threat scenario data protection and security included, of course.

Since April 2016, the former Dolphin Systems AG based in Wollerau has belonged to the F24 Group and was renamed F24 Schweiz AG in October 2019. With eCall, the company has more than 25 years of experience in implementing telecom and IT solutions on the Swiss market. The eCall platform offers solutions for high-volume communications of critical to confidential content in the business environment.

For additional information, please contact us at any time via our website www.f24.com.

F24 WWW.F24.COM

F24 Schweiz AG
Samstagernstrasse 45
8832 Wollerau, Schweiz

T +41 44 787 30 70
F +41 44 787 30 71
office_ch@f24.com