29.05.2026

Phishing is becoming ever more cunning: How “Man in the middle” attacks circumvent even MFA

Cyber-criminals continuously keep developing their phishing methods further. And so-called “man in the middle” attacks (MitM) are particularly dangerous. In the process, attackers interposition themselves in between a legitimate website and their victim without them realising, allowing the fraudsters to capture access data in real time.

Compared to classic phishing websites, MitM attacks don’t just copy a log-in page. Their fraudulent infrastructure directly passes on every input to the correct service, while showing victims the legitimate website. This is why people often don’t notice these attacks. Even multi-factor authentification (MFA) can sometimes be bypassed.

Attacks are clearly on the increase

In Switzerland, the threat posed by phishing keeps growing. There is currently a particularly treacherous type of phishing doing the rounds – man in the middle phishing. Cyber-criminals increasingly employ new hosting technologies and hard-to-recognise infrastructures in the process.

This is how MitM phishing attacks work

Attacks often start with a seemingly harmless e-mail, text or WhatsApp message containing a link to a faked log-in page. If victims click on it to log in, user name, password and sometimes even the MFA code are passed on to the legitimate website in real time. At the same time, attackers obtain access to this active session.

Particularly perfidious: Many attackers use several instances of redirection and professionally designed websites to bypass security systems. Sometimes even specialised cloud services or decentralised platforms are used so that phishing pages can remain online for longer.

How private individuals and companies can protect themselves.

There is no total protection. Still, you can considerably reduce the risks:

- Critically question log-in links contained in e-mails, text or messenger notifications
- Thoroughly check the Internet address
- Use a password manager
- Apply modern MFA methods such as FIDO2 or passkey solutions if available
- Keep your operating system, browser und security software up to date at all times
- Sensitise your employees and train them regularly

It is also important to thoroughly check suspicious log-in or unexpected MFA requests. If you suddenly receive several MFA confirmations without having logged in anywhere, you should change your password straight away and ter-

minate all active sessions.

Humans remain the most important protection factor

In spite of modern security technologies, humans remain a central target of all cyber-criminals. Phishing attacks are specifically based on time pressure, trust and habits. It is therefore important to remain vigilant and apply a healthy dose of suspicion in digital everyday life.