



The scammer knows what you bought on Tuesday

Kifli.hu: a customer-service data breach and the targeted fraud risk that follows it

Made with the AI crew, reviewed by Péter · facts as of 22 October 2026 · English version of the Hungarian original

Summary

On 5 October 2026, Kifli.hu (the Hungarian online supermarket of the Czech Rohlik group) detected unauthorised access to and data downloads from its customer-service system; at the same time, a similar incident hit the Czech parent company, Rohlík.cz. Customer-service e-mails, chats and call transcripts may have leaked, along with the contact details, addresses, order numbers and basket data in them and the notes of the AI assistant. The number of people affected and the method of intrusion are not known. The main risk is personalised fraud built on the real leaked details. The most important action: if someone contacts you in the name of Kifli, hang up, and contact them yourself through an official channel.

Key findings

- Kifli.hu detected the unauthorised access on 5 October 2026 and stopped it the same day; it notified customers on 11 October.
- In Hungary, chats and call transcripts since 21 April 2026 and e-mails since 8 July are affected, together with basket data and the AI assistant's notes.
- A similar incident happened at the Czech Rohlík.cz at the same time; there, the login and payment systems were explicitly ruled out, and the case was reported to the Czech authorities.
- The number of people affected, the method of intrusion and the perpetrator are not known; as of 22 October there is no public report of an actual fraud wave.
- The customer-service system is one of a company's most valuable data stores: context (who ordered what, and when) enables more convincing fraud than a password.

What happened

On 5 October 2026, Kifli.hu (the Hungarian online supermarket of the Czech Rohlik group) detected unauthorised access to and data downloads from its internal customer-service system. According to the company, it stopped the access the same day and fixed the flaw; it notified the affected customers by e-mail on 11 October 2026. **Confirmed** (the company's customer letter and several consistent press reports: [Index](#), [Infostart](#), [Portfolio](#), [Origo](#); all in Hungarian).

The same weekend, the group's Czech company, Rohlík.cz, also announced that data had been downloaded from its customer-service tool ([Forbes Česko](#), [Aktuálně.cz/ČTK](#)). According to the Hungarian reports, "the investigation revealed" that Hungarian customers may also be affected ([Infostart](#), [Világgazdaság](#)). The company has not said publicly whether the two cases are the same intrusion; the identical timing and description suggest so. **Assumption.**

What may have leaked (Hungary, based on the company's letter):

- e-mails sent to customer service since 8 July 2026;
- transcripts of chats and phone calls since 21 April 2026, both with staff and with the virtual assistant;
- files uploaded to the conversations;
- the names, e-mail addresses, phone numbers, delivery addresses and order numbers in them;
- data on products recently added to or removed from the basket;
- short notes by the virtual assistant.

Confirmed (Infostart, Index, Portfolio, Dívány).

What is not affected: according to the Czech company, the login and payment systems were not compromised, and the app and web shop work normally ([Forbes Česko](#), [Aktuálně.cz](#)). The Hungarian statement does not say this in the same form, only that a customer-service system is involved, not the full customer database. **Reported** (for Hungary).

What is not known: the number of people affected (neither Hungary nor the Czech Republic has published it), the method of intrusion, whether the tool was built in-house or provided by a third party, and who is behind the attack.

Timeline

Date	Event	Source
1 April 2026	Start of the affected Czech chat conversations (CZ)	czechcyber.tv , Mobilizujeme – reported
21 April 2026	Start of the affected Hungarian chats and call transcripts (HU)	Infostart, Index – confirmed
8 July 2026	Start of the affected Hungarian customer-service e-mails (HU)	Infostart, Portfolio – confirmed
5 October 2026	The company detects the unauthorised access and data download and stops it the same day	Infostart, Origo, Index – confirmed
11 October 2026	Customer letters in Hungary and the Czech Republic; Hungarian press reports (following HVG)	Infostart, Origo, Mobilizujeme – confirmed
11–12 October 2026	The Czech company reports the case to the Czech cyber security authority (NÚKIB) and the data protection authority (ÚOOÚ)	Forbes Česko, Aktuálně.cz, Expats.cz – confirmed
22 October 2026	No public news of an actual fraud wave, regulatory proceedings or the number of people affected	own search – reported

Actors and background

- **Kifli.hu:** online grocery retailer, part of the Czech Rohlik group ([Economyx](#)). According to Origo, it was the second-largest online retailer in Hungary in 2024.

- **Rohlik group:** Czech online supermarket operating in several countries (in Germany under the name Knuspr). Customer-service data also leaked at the Czech company; there are no public reports from other markets (Germany, Austria, etc.). **Reported.**
- **Precedent and pattern:** the customer-service system as a target is not new. On 3 October 2025, Discord announced that, through an external customer-service partner, attackers had accessed support conversations and the ID photos of about 70,000 users, and demanded a ransom ([Discord](#), [Bitdefender](#)). According to Origo, there is no documented precedent for a customer-service incident of this scale in Hungarian online retail.

How it works (Red // attacker's view)

- **Customer service is the company's "diary".** This is where the customer writes what was missing from the delivery, when they ordered, and where they want it delivered – and sometimes things that do not belong there (a password, card details). The Czech company itself said that some customers had shared passwords or card details in conversations, and notified them separately ([Expats.cz](#)).
- **The value is the context, not the password.** From the real details (order number, missing product, earlier complaint, basket contents), the scammer builds a convincing pretext: a refund, a customer-service callback, a code request because of a "suspicious login". The company itself warned about this: scammers may pose as customer service or as staff handling a refund ([Dívány](#)).
- **The virtual assistant is a data store too.** The AI assistant's notes summarise what the customer wanted – for an attacker, that is a ready-made script.
- **The trick is psychological.** The real detail switches off suspicion, and the urgency leaves no time to think.

Impact and the Hungarian angle

- **Directly affected:** Kifli.hu customers who contacted customer service by chat or phone since 21 April 2026, or by e-mail since 8 July. Their number is not known.
- **Indirect risk:** personalised phishing e-mails, text messages and calls in the company's name, possibly weeks or months later. The company itself warns about this.
- **Authorities:** the Czech company reported the case to the Czech authorities. There is no public information about a report to, or proceedings by, the Hungarian data protection authority (NAIH). Under the GDPR, a serious incident must be reported to the supervisory authority within 72 hours, so a report is likely but not confirmed. **Open.**
- **Fraud wave:** as of 22 October 2026, there is no public report of an actual fraud wave built on the leaked data. **Reported (absence).**

What to do (Blue // what to do now)

Individual (Kifli customer):

1. If someone calls or writes in the name of Kifli, hang up / do not reply, and contact them through the app or by typing the kifli.hu address yourself.
2. Do not click links received in messages, and do not install anything for a "refund".

3. Never give a password, online banking details, your card's security code or an SMS code in response to an unsolicited call or message.
4. If you have ever written a password to customer service, change it – everywhere you use the same one.
5. If you have given bank details, tell your bank immediately.
6. Tell your parents and grandparents: they get the most convincing calls.

Small business (web shop, service provider):

1. Check what your customer-service system stores (chat, e-mail, call transcripts) and for how long – set a retention period.
2. Turn on automatic masking of card-number and password patterns, if the system supports it.
3. Tell your customers openly: "this is how we contact you, and this is how we never do".
4. Ask your provider who has access to the system (staff, external partners, AI integrations).

Organisation:

1. Treat the customer-service platform (ticketing, chat, call recording, AI assistant) as a high-value data store: access management, MFA, logging, anomaly monitoring.
2. Data minimisation: short retention, masking, removing sensitive data.
3. Supplier risk: regular review of the access of external customer-service partners and integrations, with the ability to revoke it quickly.
4. Incident communication template: with concrete "this is how we contact you / this is how we don't" sentences, naming the official channels.

Technical block

- **CVE / affected product:** not known; the company has named neither the system nor the vulnerability.
- **Likely MITRE ATT&CK techniques (for the consequences, not the intrusion):** T1598 / T1566 (phishing with the leaked context), T1656 (impersonation). The intrusion technique is not known.
- **Detection ideas (for customer-service platforms):** monitoring of bulk exports or API queries, agent logins at unusual times or from unusual locations, new integration tokens or apps, large volumes of attachment downloads.
- **Official recommendations:** the company's recommendations (see Blue). The Czech authorities (NÚKIB, ÚOOÚ) received reports but have not published recommendations on the case.
- **Indicators:** none published.

Contradictions and open questions

- **Different periods:** according to the Czech reports, chats there date from 1 April to 5 October 2026, call transcripts from 28 April to 5 October, and e-mails from 28 June to 22 September; in Hungary, since 21 April (chat, calls) and since 8 July (e-mail). The reason for the difference is not known (different roll-out, different retention?).
- **One incident or two?** It has not been stated that the Hungarian and Czech cases are the same intrusion.
- **Login and payment:** explicitly ruled out in the Czech Republic; no such statement has appeared in Hungary.

- **Number of people affected, method of intrusion, role of a third-party provider, perpetrator:** not known.
- **Report to the Hungarian authority:** no public information.
- **Actual fraud:** no public reports as of 22 October.

Source assessment

Source	Type	Reliability	What it supports
Infostart (HU)	press (based on the company's statement)	high	dates, data categories, recommendations
Index (HU)	press	high	dates, data categories, recommendations
Portfolio (HU)	press (following HVG)	high	data categories, customer letter
Origo (HU)	press	medium	dates, market position, absence of precedent
Dívány (HU)	press	medium	the company's warning about impersonation
Világgazdaság (HU)	press	medium	Hungarian exposure following the investigation
Forbes Česko (CZ)	press (ČTK, company statement)	high	Czech case, report to authorities, login/payment not affected
Aktuálně.cz (CZ)	press (ČTK)	high	company statements, authorities
Expats.cz (EN)	press	medium	separate notification of customers who shared passwords/card data
czechcyber.tv (CZ)	trade press	medium	Czech periods
Mobilizujeme (CZ)	press	medium	Czech periods, basket data
Brandsit (EN)	press	medium	AI assistant notes
Economx (HU)	background	medium	Rohlik parent company
Discord (EN)	company	high	precedent: via a customer-service partner
Bitdefender (EN)	researcher/press	medium	figures of the Discord precedent

promptlysecured.com · Changelog: first revision (v1), no changes. · The Hungarian original is the reference version.