

Medienmitteilung – Sicherheitsvorfall quitt (7. Oktober 2026)

Sicherheitsvorfall bei quitt: Profildaten von Arbeitnehmenden unrechtmässig kopiert

Medienmitteilung | Zürich | 14. Oktober 2026

- Am 7. Oktober 2026 hat eine unberechtigte Drittperson gefälschte Arbeitgeber Profile erstellt über eine veraltete, nicht mehr genutzte technische Schnittstelle Profildaten von rund 29'800 Arbeitnehmenden kopiert, die aktuell oder in der Vergangenheit über quitt in Schweizer Privathaushalten angestellt waren. Darunter befinden sich teilweise Angaben wie AHV-Nummer, Geburtsdatum, E-Mail, Adresse und IBAN.
- Nicht betroffen sind Lohndaten, Arbeitsverträge, Dokumente, Passwörter und Gesundheitsdaten sowie sämtliche Daten der Arbeitgebenden. Es wurden keine Daten verändert oder gelöscht. quitt Business, quitt Deutschland und quinn UK sind nicht betroffen.
- Die Sicherheitslücke ist geschlossen. quitt hat den Vorfall dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) und dem Bundesamt für Cybersicherheit (BACS) gemeldet, Strafanzeige eingereicht und, soweit möglich, die betroffenen Arbeitnehmenden persönlich informiert.

Was passiert ist

Am Nachmittag des 7. Oktober 2026 meldeten sich Arbeitnehmende beim quitt Support, weil sie unerwartete Einladungen erhalten hatten. Eine erste Abklärung ergab, dass eine unberechtigte Drittperson auf der quitt Plattform automatisiert rund hunderte gefälschte Arbeitgeber-Konten erstellt und darüber zehntausende Einladungs-Nachrichten verschickt hatte. quitt schaltete die Einladungsfunktion und den SMS-Versand noch am selben Tag ab und löschte die gefälschten Konten.

quitt ging zunächst von einem Vorfall mit geringer Tragweite aus. Die vertiefte Analyse der Zugriffsprotokolle in den folgenden Tagen zeigte jedoch, dass über eine veraltete Schnittstelle aus einer früheren Version der Plattform Profildaten von Arbeitnehmenden im grossen Umfang kopiert worden waren. Am 12. Oktober lag die Bestätigung vor, dass davon ausgegangen werden muss, dass die Daten von rund 29'800 Arbeitnehmenden – rund 80 Prozent der in der Datenbank registrierten Arbeitnehmenden – kopiert wurden.

Der Vorfall betrifft ausschliesslich der Plattform von quitt für Privathaushalte in der Schweiz. Die Systeme von quitt Business, quitt Deutschland und quinn UK sind getrennt und nicht betroffen.

Welche Daten betroffen sind – und welche nicht

Kopiert wurden Profildaten von Arbeitnehmenden, soweit diese im Profil hinterlegt waren: Name, Kontaktangaben (E-Mail-Adresse, Telefonnummer), Adresse, Geburtsdatum, AHV-Nummer, Aufenthaltsstatus sowie bei rund der Hälfte der Betroffenen die IBAN. Aufgrund gesetzlicher Pflichten sind auch ehemalige Arbeitnehmende betroffen, deren Daten über das Arbeitsverhältnis hinaus aufbewahrt werden müssen.

Nicht betroffen sind Lohndaten, Lohnabrechnungen, Arbeitsverträge, hochgeladene Dokumente wie Kopien von Pass oder ID sowie Passwörter und Gesundheitsdaten. Ebenfalls nicht betroffen sind sämtliche Daten der Arbeitgebenden. Es wurden keine Daten verändert oder gelöscht; es handelt sich um einen reinen Datenabfluss. Die Nutzung der Website und des Kundenbereichs war zu keinem Zeitpunkt gefährdend.

Was quitt unternommen hat

Die Sicherheitslücke ist geschlossen. quitt hat die missbrauchten und nicht mehr genutzten Schnittstellen vollständig entfernt, die Prüfung aller eingehenden Daten verschärft und einen Captcha-Schutz gegen automatisierte Kontoerstellung eingeführt. Änderungsanträge an Personendaten werden bis auf Weiteres nicht

mehr automatisch verarbeitet, sondern geprüft. Ein weiterer versuchter Angriff am 8. Oktober verlief erfolglos. Seit dem 9. Oktober wurde kein weiterer Zugriff festgestellt.

quitt hat den Vorfall dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) und dem Bundesamt für Cybersicherheit (BACS) gemeldet und bei der Polizei Strafanzeige gegen Unbekannt eingereicht. Das Unternehmen wird durch eine auf Datenschutz spezialisierte Anwaltskanzlei begleitet und folgt den Empfehlungen der Aufsichtsbehörde.

Seit dem Abend des 13. Oktober informiert quitt alle betroffenen Arbeitnehmenden persönlich. Die Information enthält konkrete Hinweise, worauf Betroffene jetzt achten sollten. Ausführliche Informationen sind im Helpcenter von quitt abrufbar; Fragen beantwortet der quitt Support unter support@quitt.ch oder 043 505 18 02 (Mo–Fr, 9–13 Uhr).

Parallel überprüft quitt seine gesamte Sicherheitsarchitektur. Weitere Massnahmen wie Zugriffsbegrenzungen auf allen Schnittstellen und externe Penetrationstests sind in Vorbereitung.

«Dieser Vorfall tut uns sehr leid. Arbeitnehmende und Arbeitgebende vertrauen uns ihre Daten an, und diesem Vertrauen sind wir hier nicht gerecht geworden. Wir haben die Lücke geschlossen, die Behörden eingeschaltet und alle Betroffenen informiert. Jetzt sorgen wir dafür, dass sich so etwas nicht wiederholt», sagt David Christen, CEO von ServiceHunter AG.

Was betroffene Arbeitnehmende jetzt tun sollten

Die kopierten Daten eignen sich für Phishing-Versuche, die sehr echt wirken können, weil sie Name, Adresse oder AHV-Nummer enthalten. quitt empfiehlt Betroffenen:

- Vorsicht bei unerwarteten Nachrichten, die zum Klick auf einen Link, zum Öffnen eines Anhangs, zu einer Zahlung oder zur Bestätigung persönlicher Daten auffordern – auch wenn sie scheinbar von quitt, der Arbeitgeberin, der Bank oder einer Behörde stammen. quitt fragt nie per E-Mail nach Passwörtern oder Bankdaten.
- Absenderadressen genau prüfen und im Zweifel nicht antworten, sondern die Organisation über selbst nachgeschlagene Kontaktangaben direkt kontaktieren.
- Kontoauszüge in den kommenden Wochen aufmerksam prüfen und verdächtige Buchungen sofort der Bank melden. Mit der IBAN allein kann niemand Geld vom Konto abheben; sie kann aber für Betrugsversuche missbraucht werden.
- Rechnungen, Mahnungen oder Verträge für nicht bestellte Leistungen beim Absender und, falls nötig, bei der Polizei melden.

Ein Passwortwechsel ist wegen dieses Vorfalls nicht nötig; Passwörter waren nicht betroffen.

Über ServiceHunter AG

ServiceHunter AG ist das Zürcher Unternehmen hinter quitt, quitt Business und quinn: ein app-basierter, automatisierter Service für Lohn- und Anstellungsadministration für Privathaushalte und Unternehmen, die Personen direkt anstellen. Für Privathaushalte übernimmt quitt die korrekte Anstellung von Haushaltshilfen wie Reinigungskräften, Nannys, Betreuungspersonen und Gärtnerinnen; für Unternehmen führt quitt Business die Lohn- und Personaladministration, ohne dass Kundinnen und Kunden Lohnsoftware bedienen oder ein Treuhandbüro koordinieren müssen. Die Kundin bleibt Arbeitgeberin; quitt handelt in ihrem Auftrag und übernimmt Anmeldungen, Lohnabrechnung, Zahlungen, Versicherungen, Pensionskasse, Steuern und Meldungen – automatisiert, von A bis Z. ServiceHunter AG ist seit 2002 tätig, operiert in der Schweiz, Deutschland und Grossbritannien und hat für über 50'000 Arbeitgebende mehr als CHF 1,5 Milliarden Lohnsumme abgerechnet.

Kontakt für Medien

Luna Arnold
Marketing
luna.arnold@quitt.ch

ServiceHunter AG – quitt
Birmensdorferstrasse 94
8003 Zurich, Switzerland

www.quitt.ch
www.quitt.business
www.go-quitt.de
www.quinn.uk