LANDESKRIMINALAMT
NIEDERSACHSEN

Landeskriminalamt Niedersachsen
Dezernat FPJ –
Forschung | Prävention | Jugend
Zentralstelle Prävention

Landeskriminalamt Niedersachsen | Postfach 38 60 | 30038 Hannover

Bearbeitet von
Henschel, KHK

E-Mail
praevention@lka.polizei.niedersachsen.de

Hannover
18.11.2026

Dringende Warnung vor aktueller Phishing-Betrugsmasche im Namen der apoBank

Sehr geehrte Damen und Herren,

das Landeskriminalamt Niedersachsen warnt aktuell vor einer gezielten Betrugsmasche, bei der insbesondere Ärztinnen und Ärzte, Zahnärztinnen und Zahnärzte sowie Apothekerinnen und Apotheker ins Visier genommen werden.

Die Täter versenden gefälschte Schreiben im Namen der Deutschen Apotheker- und Ärztebank (apoBank) per Briefpost. Darin werden die Empfängerinnen und Empfänger unter einem Vorwand aufgefordert, einen beigefügten QR-Code zu scannen, beispielsweise um vermeintlich notwendige Aktualisierungen vorzunehmen. Der QR-Code führt auf eine gefälschte Internetseite, auf der sensible Zugangsdaten abgegriffen werden sollen.
Zusätzlich nutzen die Täter teilweise E-Mails und telefonische Kontakte, um ihre Vorgehensweise glaubwürdiger erscheinen zu lassen und das Vertrauen der Betroffenen zu gewinnen. Ziel ist es, an Zugangsdaten zu gelangen und diese anschließend für unberechtigte Transaktionen zu missbrauchen.

Bereits mehrere Fälle und erhebliche Schäden in Niedersachsen

Die Betrugsmasche ist auch in Niedersachsen angekommen. Dem Landeskriminalamt liegen bereits mehrere angezeigte Fälle vor. Die bislang bekannt gewordenen Schadenssummen bewegen sich insgesamt bereits in Einzelfällen im unteren sechsstelligen Eurobereich. Es ist davon auszugehen, dass weitere Praxen und Apotheken betroffen sein könnten.

Wie können Sie sich schützen?

- Scannen Sie QR-Codes in unerwarteten Schreiben nicht ungeprüft. Kontrollieren Sie insbesondere, wohin der QR-Code tatsächlich führt.
- Geben Sie niemals Zugangsdaten, PIN oder TAN auf Internetseiten ein, die Sie über einen QR-Code oder einen Link aus einer unerwarteten Nachricht aufgerufen haben.
- Lassen Sie sich auch durch zusätzliche telefonische Kontakte oder E-Mails nicht unter Druck setzen. Beenden Sie im Zweifel das Gespräch und nehmen Sie selbstständig über bekannte und vertrauenswürdige Kontaktdaten Verbindung zu Ihrer Bank auf.

- Prüfen Sie verdächtige Schreiben und Aufforderungen zur Aktualisierung von Zugangsdaten unmittelbar über die offiziellen Kontaktwege Ihrer Bank.
- Informieren Sie auch Ihre Mitarbeitenden für den Umgang mit entsprechenden Schreiben, E-Mails und Anrufen. Gerade in Praxis- und Apothekenbetrieben kann eine frühzeitige Sensibilisierung dazu beitragen, Schäden zu verhindern.

Weitere Informationen und konkrete Hinweise

Eine ausführliche Beschreibung der aktuellen Betrugsmasche sowie weitere Verhaltensempfehlungen finden Sie in der Warnmeldung des Landeskriminalamtes Niedersachsen:

https://www.polizei-praevention.de/aktuelles/qr-code-phishing-quishing-per-briefpost-im-namen-der-apobank-auch-in-kombination-mit-anrufen-und-mails.html

Sollten Sie bereits Zugangsdaten auf einer verdächtigen Internetseite eingegeben haben, kontaktieren Sie unverzüglich Ihre Bank über die offiziellen Kontaktwege, veranlassen Sie die Sperrung betroffener Zugänge und lassen Sie gegebenenfalls weitere Zahlungsmaßnahmen prüfen.

Erstatten Sie zudem Anzeige bei ihrer örtlichen Polizei.

Bitte nehmen Sie diese Warnung ernst und informieren Sie auch Ihre Mitarbeiterinnen und Mitarbeiter.
Eine frühzeitige Sensibilisierung kann dazu beitragen, weitere Betrugsfälle und finanzielle Schäden zu verhindern.

Mit freundlichen Grüßen

Henschel, Kriminalhauptkommissar

Landeskriminalamt Niedersachsen
Dezernat Forschung | Prävention | Jugend
Zentralstelle Prävention