

Identitätsbetrug !!!

Sie sind einem Phishing-Angriff erlegen. Auf eine eMail Ihrer „Bank“ haben Sie zur angeblichen Verifizierung Ihrer Person **(bei diesem Begriff läuten bei mir alle Alarmglocken)** neben persönlicher Daten, wie Übermittlung des PA, Bankdaten wie IBAN, Passwörter, „Foto-TAN“ usw. preisgegeben. Damit nimmt der Betrüger Ihre Identität an. Seine erste Handlung wird die Änderung Ihres Passworts als Zugang zu Ihrem Online-Konto sein. Er sperrt Sie aus, damit er in Ruhe Ihr Konto abräumen kann. Im nächsten Schritt tätigt er z.B. Bestellungen mit einem Weiterleitungsvermerk. Die Rechnungen gehen an Sie. Mahnungen! Im Gefolge werden Inkasso-Unternehmen und Gerichte bemüht. Auch Anlage neuer Konten, Kreditanträge sind möglich, aber wohl schwieriger zu erlangen. **In allen Fällen sind Sie beweispflichtig** und wissen nichts von den Machenschaften des Betrügers. Ihre Daten können auch im DarkNet zur weiteren Verfügung verkauft werden. Es ist beunruhigend, wenn Sie feststellen, Opfer eines Identitätsbetrugs geworden zu sein. Im Extremfall kann sogar Ihre ganze Existenz gefährdet sein. **Deshalb informieren Sie unverzüglich Ihre Bank und erstatten umgehend Anzeige bei der Kriminalpolizei!!!**

Auf jeden Fall werden Sie mindestens unheimlichen Ärger und evtl. finanzielle Einbussen über Schadensersatzforderungen haben.

Kartenzahlung und Kartendiebstahl

Kartenzahlung über Kartenlesegerät oder NFC

Feste Regelungen zur Abfrage der PIN bei Kartenzahlungen in der Europäischen Union festgelegt. Dabei gilt zunächst, dass man den **Code** immer dann eingeben muss, wenn die **Geldkarte in das Kartenlesegerät** gesteckt wird.

In der Praxis passiert das immer seltener, denn die allermeisten Girokarten verfügen inzwischen über einen sogenannten **NFC-Chip** für das Bezahlen **durch Auflegen**. Für diese Art des Bezahlens gelten dann andere Regeln: „Bei Beträgen bis zu 50 Euro wird in der Regel nie eine PIN verlangt.“ Wer **bis zu fünf Bezahlvorgänge** mit einer Gesamtsumme von 150 Euro abwickelt, müsse ebenfalls keine PIN eingeben.

Unterschiede:

Sofortabbuchung bei PIN-Zahlung und 0,2% des Rechnungsbetrages. Bei Unterschrift wird der Bezahlvorgang wie eine „Einzugsermächtigung, also später erfolgen.

Wie sichere ich mich gegen Kartendiebstahl

Die Polizei rät: Kleben Sie einen Sticker mit einer **falschen PIN** auf Ihre Bankkarte. Auf diese Weise irritieren Sie potenzielle Diebe im besten Fall so sehr, dass sie die in-korrekte Zahl dreimal eingeben und Ihre Karte am Automaten eingezogen wird. Dann haben Sie zwar etwas bürokratischen Aufwand, Ihr Geld ist aber zumindest in Sicherheit

05.12.2024

Debit- oder Master-Karte verloren oder gestohlen? Achten Sie auf diese Schritte

Karte sofort sperren:

- Bei Ihrer Bank (Filiale, Hotline oder App)
- Oder beim bundesweiten Sperrdienst 116 116

PIN-Sperre schützt nur vor Bargeldabhebungen,
nicht vor SEPA-Lastschriften.

Kriminalitätsbekämpfung im unbaren Zahlungsverkehr unter Nutzung nicht personalisierter Zahlungskarten

KUNO beantragen:

KUNO-Sperre nur gegen unautorisierte Lastschriften:

- **Nur persönlich bei der Polizei aktivierbar**
 - Online, oder telefonisch nicht möglich

Mit Bank- und KUNO-Sperre sind sowohl

Abhebungen als auch Lastschriften gestoppt.

10 Milliarden Passwörter geleakt – So prüfen Sie, ob Ihre Daten betroffen sind

Passwort gehackt? Mit diesem Check finden Sie es heraus:

Im Juli diesen Jahres sind durch den wohl größten Leak aller Zeiten rund **10 Milliarden Klartextpasswörter** ins Netz gelangt. Noch immer gibt es Betroffene, die nicht wissen, ob ihr Passwort kompromittiert wurde. Wir erklären Ihnen, wie Sie überprüfen, ob Ihr Account betroffen ist und was jetzt zu tun ist. Überprüfen Sie Ihre Konten regelmäßig auf ungewöhnliche Aktivitäten. Das können zum Beispiel Anmeldungen von ungewöhnlichen Orten oder Geräten sein, die Sie nicht erkennen. Erhalten Sie E-Mails von Online-Diensten über Änderungen an Ihren Kontoeinstellungen, die Sie nicht selbst vorgenommen haben? Das könnte darauf hinweisen, dass jemand unbefugt auf Ihr Konto zugegriffen hat. Wenn Sie sich plötzlich nicht mehr in Ihre Konten einloggen können, obwohl Sie sicher sind, dass Sie die richtigen Anmeldeinformationen verwenden, sollten Sie alarmiert sein. Dies könnte darauf hindeuten, dass jemand Ihr Passwort geändert hat.

Auf der Seite des Hasso-Plattner-Instituts finden Sie den [Identity Leak Checker](#). Hier können Sie Ihre E-Mail-Adresse angeben und so prüfen, ob diese oder andere sensible Daten gehackt wurden und im Netz verfügbar sind.

Betroffener Dienst	Datum	Verifiziert	Betroffene Nutzer	Passwort	Vor- und Zuname	Geburtsdatum	Anschrift	Telefonnummer	Kreditkarte	Bankkontodaten	Sozialversicherungsnr.	IP-Adresse
Online Spambot (Spamlist)	Aug. 2017		128.471.704	–	–	–	–	–	–	–	–	–
adobe.com	Okt. 2013	✓	152.375.851	–	–	–	–	–	–	–	–	–
dropbox.com	Sep. 2012	✓	68.658.165	Betroffen	–	–	–	–	–	–	–	–

Ergebnisse für [REDACTED]@t-online.de

Datenleaks

Wir haben Ihre E-Mail-Adresse in folgenden Datenleaks gefunden. Bitte stellen Sie sicher, dass die betroffenen Passwörter weder verwendet noch an anderer Stelle wiederverwendet werden:

	Betroffene Daten										Verifiziert?	Leak-Datum	Passwort geändert?
	IP	Bankdaten	Kreditkarte	Name	Passwort	Ausweis	Tel.-Nr.	Benutzername	Geburtsdatum	Adresse			
adobe.com	-	-	-	-	-	-	-	-	-	-	✓	04.10.2013	☐
dropbox.com	-	-	-	-	✓	-	-	-	-	-	✓	21.09.2012	☐
Onliner Spambot (Spamlist)	-	-	-	-	-	-	-	-	-	-	X	30.08.2017	☐
brillen.de	-	-	-	✓	-	-	✓	-	✓	✓	✓	25.02.2026	☐

Infostealer



Wir haben Ihre E-Mail-Adresse in keinem uns bekanntem Infostealer-Log von Malware gefunden.