

## Datenleck beim Mastercard Bonus-Programm "Priceless Specials" - Was Betroffene jetzt tun sollten

Freitag, 23 August 2019

<https://www.datenschutz.de/datenleck-beim-mastercard-bonus-programm-priceless-specials-was-betroffene-jetzt-tun-sollten/>

Pressemitteilung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz vom 23.08.2019

Am 19. August 2019 wurde bekannt, dass Daten aus dem Mastercard-Bonusprogramm „Priceless Specials“ von der Plattform eines Dienstleisters abgegriffen wurden. Nach den bislang vorliegenden Informationen handelte es sich dabei um ca. 90.000 Datensätze mit Namen, Email-Adressen, Anschriften, Geburtsdaten, Telefonnummern sowie teilweise verschlüsselte Kreditkartennummern.

Darüber hinaus kursiert eine weitere Liste mit vollständigen Kreditkartennummern, deren Herkunft bislang jedoch unklar ist.

Der Vorfall zeigt nach Ansicht des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, Prof. Dr. Dieter Kugelmann, einmal mehr, wie weit die Digitalisierung das persönliche Lebensumfeld durchdringt und wie schnell sich Sicherheitsrisiken manifestieren können. „Das Risiko eines Datenlecks muss immer in die Überlegungen einbezogen werden, ob und wie man Dienste der Informationsgesellschaft nutzt. Gerade auch beim Einsatz von Dienstleistern außerhalb direkter Einwirkungsmöglichkeiten des Verantwortlichen muss durchgängig eine verlässliche IT-Sicherheit gewährleistet werden.“

Der Landesbeauftragte rät den Inhabern einer Mastercard, insbesondere aber den Teilnehmern des Bonusprogramms, sich danach zu erkundigen, ob sie von der aktuellen Datenpanne betroffen sind. Dies kann z.B. über den [HPI Identity Leak Checker](#) des Hasso-Plattner-Instituts in Potsdam geprüft werden. Hierzu wird die Mailadresse benötigt, mit der man sich beim Bonusprogramm registriert hat.

Betroffene Teilnehmer des Bonusprogramms sollten umgehend Kontakt mit Mastercard aufnehmen, um die nächsten Schritte zu klären. Unabhängig davon sollte auf Unregelmäßigkeiten bei Abbuchungen und in den Kreditkartenabrechnungen geachtet werden.

Häufig werden erbeutete Daten für sogenannte Phishing Attacken genutzt, um über vorliegende Kontaktdaten an weitere Informationen und Zugangsdaten zu gelangen. Die Teilnehmer des Bonusprogramms sollten daher verstärkt auf ungewöhnliche Kontaktversuche achten und bei Nachrichten – egal ob per Mail, SMS oder Messenger – prüfen, ob der Absender bekannt ist. Insbesondere sollten E-Mail-Anhänge und angebotene Internet-Links nicht unbedacht angeklickt werden.

Mastercard unterhält in Hessen eine deutsche Repräsentanz. Daher koordiniert der Hessische Beauftragte für Datenschutz und Informationsfreiheit die Bearbeitung der Datenschutzanfragen in Deutschland.

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit

Postfach 3163

65021 Wiesbaden

Telefon: 0611-1408 0

Telefax: 0611-1408 611

E-Mail: [poststelle\(at\)datenschutz.hessen.de](mailto:poststelle(at)datenschutz.hessen.de)

Internet: <https://datenschutz.hessen.de>

Seinen europäischen Hauptsitz hat Mastercard in Belgien. Zuständige Aufsichtsbehörde ist die

Commission de la Protection de la Vie Privée

Rue de la Presse 35

1000 Brussels

Telefon: +32 (0) 2 274 48 00

Telefax: +32 (0) 2 274 48 35

E-Mail: [commission\(at\)privacycommission.be](mailto:commission(at)privacycommission.be)

Internet: <https://www.privacycommission.be>

Weitere Informationen:

- [Pressemitteilung des Hessischen Datenschutzbeauftragten](#)
- [Informationen der Verbraucherzentralen zum Thema Identitätsdiebstahl](#)

Die Pressemitteilungen des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz [können hier abgerufen](#) werden.