Datenschutz „leicht gemacht“ - Einfache Tipps zum Schutz persönlicher Daten im Internet

Datenschutz im Internet ist und bleibt ein topaktuelles Thema. Das zeigen auch die Ergebnisse des ERGO Risiko-Reports: Über die Hälfte der Befragten fürchten sich vor dem Missbrauch persönlicher Daten. Dennoch nutzen beispielsweise zwei von zehn Deutschen öffentliches WLAN für Bankgeschäfte. Dieter Sprott, Experte der ERGO Direkt Versicherungen, erklärt, wie einfache Maßnahmen helfen, die eigenen Daten im Netz besser zu schützen.

Das A und O des Datenschutzes: das Passwort
Laut ARD/ZDF-Onlinestudie lag im Jahr 2017 die durchschnittliche tägliche Dauer der Internetnutzung bei 149 Minuten. Wer so viel surft, hat in der Regel auch eine Vielzahl von Accounts – für das Online-Banking, bei Shopping-Portalen oder bei Streaming-Diensten. Alle müssen mit einem Passwort geschützt werden. Warum also nicht einfach „123456“ – alle Jahre wieder das am häufigsten gewählte Passwort – für sämtliche Konten verwenden? „Ein einziges Passwort und noch dazu ein sehr einfaches macht es Hackern äußert leicht, den Zugang zu knacken“, gibt Dieter Sprott zu bedenken. Da das Passwort meistens der einzige Schutz für private Daten ist, empfiehlt sich etwas mehr Aufwand. Der Rat des ERGO Direkt Experten: „Wer online unterwegs ist, sollte sich die Zeit nehmen, für jeden Account ein individuelles, sicheres Passwort festzulegen. Passwörter sollten 12 Zeichen lang sein und Buchstaben, Zahlen und Sonderzeichen enthalten. Wichtig ist zudem: Die Passwörter regelmäßig ändern! Das tut laut ERGO Risiko-Report nur etwa jeder Dritte. Zugegeben: Den Überblick über die zahlreichen Varianten zu behalten, ist schwer. Daher der Tipp von Sprott: Einen sogenannten Passwort Manager verwenden. Dieses Tool speichert sensible Daten wie Nutzernamen und Passwörter verschlüsselt in einer Datenbank auf der Festplatte des Anwenders. Um darauf zugreifen zu können, benötigt der Nutzer dann nur ein einziges Passwort, das Master-Passwort. Kostenlose Passwort Manager finden Anwender in großer Zahl im Internet.

Vorsicht vor Daten-„Phishern“
Dem Identitätsmissbrauch geht meist der Identitätsdiebstahl voraus. Dafür verschicken Internetbetrüger sogenannte „Phishing“-Mails, die als offizielle Mitteilung einer Bank, einer vertrauten Person oder eines Online-Shops getarnt sind. Meist fragen die Betrüger darin vertrauliche Informationen wie Passwörter oder Transaktionsnummern ab. „Damit kaufen sie dann im Namen der Betroffenen online ein oder heben Geld von ihrem Konto ab“, erklärt Sprott. Die „Phishing“-Mails sind mittlerweile sehr professionell gestaltet und sehen denen des echten Absenders oft täuschend ähnlich. Dennoch können Verbraucher sich schützen. Wichtig ist, grundsätzlich skeptisch gegenüber einer Abfrage persönlicher Daten per Mail zu sein. Im Zweifelsfall dann die einfachste Möglichkeit: Die Mail löschen. „Sollte dabei eine echte Anfrage untergehen, wird sich der Absender sicher wieder melden“, so der ERGO Direkt Experte. Keinesfalls sollten sich die Empfänger verleiten lassen, mitgeschickte Anhänge oder Links zu öffnen. „Oft reicht bereits ein Klick, damit sich auf dem Computer eine Spyware oder ein Virus installiert“, warnt Sprott. Wer es genauer wissen will, kann beim Kundenservice des betreffenden Unternehmens anrufen. Ob die Mail echt ist oder nicht, werden die Mitarbeiter dort klären können. Was viele User nicht wissen: In der Regel senden seriöse Unternehmen weder Mahnungen per E-Mail, noch würden sie Kunden in einer E-Mail zur Angabe von Passwörtern, PINs oder TANs auffordern. Erscheint die Mail einer vertrauten Person seltsam, am besten den Betreffenden kurz kontaktieren, ob er wirklich der Absender ist. Übrigens: Im öffentlichen WLAN ist besondere Vorsicht geboten! „Für Cyberkriminelle ist es ein Kinderspiel, mit einer entsprechenden Software in das Netz einzudringen und Nachrichten oder Zugangsdaten

beispielsweise mitzulesen“, erklärt Sprott. Hier also besser keine Bankgeschäfte tätigen. Gibt es in der Auswahlliste für WLAN mehrere ähnlich lautende Einträge, sollten Nutzer laut dem Experten von ERGO Direkt beim Anbieter nach dem richtigen Zugang fragen. Denn Betrüger stellen oft Hotspots zur Verfügung, die dem Original ähneln, um so an die Daten zu kommen.

Unterwegs in den sozialen Medien: Nicht jeder muss alles wissen!

Wer Facebook & Co. nutzt, gibt – oft ungewollt oder unbewusst – viel von sich preis. Denn die sozialen Netzwerke sammeln große Mengen an Daten über die Gewohnheiten ihrer Nutzer. Daraus erstellen sie Profile, verkaufen die Daten an ihre Werbekunden oder schneiden Werbung auf den jeweiligen Anwender zu. Nicht jeder Nutzer ist damit einverstanden. Grundsätzlich hilft es, sich jeweils für die strengsten Privatsphäre-Einstellungen zu entscheiden. Zudem rät der ERGO Direkt Experte, Felder des eigenen Profils frei zu lassen – zum Beispiel Postanschrift und private Handynummer. Diese Angaben benötigt normalerweise keiner der Freunde im Netzwerk. Wichtig zu wissen: Wer sich mit seinem Facebook-Profil bei einer App oder einer Webseite anmeldet, ermöglicht diesen Diensten damit den Zugriff auf seine persönlichen Daten. In den Facebook-Einstellungen ist unter dem Punkt „Apps und Webseiten“ erkennbar, welche Apps und Webseiten mit dem Facebook-Konto verbunden sind. Der Anwender kann diese Verbindungen löschen und sich direkt bei den jeweiligen Seiten und Apps anmelden. Allerdings gilt: „Ein vollständiger Schutz der Privatsphäre im Internet ist heute nicht mehr möglich“, so Sprott. „Dafür ist die virtuelle Welt zu vernetzt. Wer hier unterwegs ist, sollte daher vorsichtig sein und mit privaten Daten sehr restriktiv umgehen.“

KONTAKT

ERGO Direkt Versicherungen
Media Relations
Tina Johanna Kunath
Tel. 0211 477-2324
tina.kunath@ergo.de