

Datenlöschen leicht gemacht: So schützen Sie Ihre Privatsphäre!

Erfahren Sie, wie Sie Daten sicher löschen können: Methoden, Softwareempfehlungen und wichtige Tipps für den Schutz Ihrer Privatsphäre.



Deutschland - Die Sorge um den Datenschutz und die sichere Löschung von Daten nimmt in der heutigen digitalen Welt einen immer höheren Stellenwert ein. Viele Nutzer sind sich jedoch nicht bewusst, dass gelöscht geglaubte Daten oft nicht vollständig entfernt sind. Diese Thematik ist besonders relevant vor dem Verkauf, der Entsorgung oder dem Ausleihen von Geräten, um ungewollten Zugriff auf persönliche Daten zu vermeiden. Die Informationen, die durch einfache Löschvorgänge wie das Leeren des Papierkorbs oder die Formatierung eines Speichermediums verfügbar bleiben, sind durchaus besorgniserregend.

Wie **FAZ** berichtet, werden beim Löschen über den Papierkorb

häufig nur die Verweise auf die Dateien entfernt, während die Daten selbst auf der Festplatte bestehen bleiben. Richtiges Löschen, das auch die Daten selbst umfasst, erfolgt erst, wenn die entsprechenden Speichersektoren überschrieben werden. Um dies zu erreichen, empfiehlt das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Verwendung spezieller Überschreib-Software, die die Daten entweder einmal oder mehrfach mit zufällig generierten Zeichen überschreibt. Diese Methode hat sich in den meisten Fällen als ausreichend erwiesen, um Daten unwiederbringlich zu löschen.

Sichere Löschmethoden

Die sicherste Möglichkeit zur Datenlöschung wird durch den Einsatz solcher Software wie „Eraser“ gewährleistet, die kostenlos zum Download angeboten wird, beispielsweise beim Heise-Verlag. Nach der Installation steht „Eraser“ im Kontextmenü zur Verfügung, um Dateien oder Ordner direkt sicher zu löschen. Zudem ermöglicht die Software das automatisierte Überschreiben bestimmter Festplattenbereiche, was eine noch gründlichere Löschung gewährleistet.

Das BSI bietet zudem verschiedene Methoden zur sicheren Datenlöschung an. Zu diesen zählen das Überschreiben der Daten mit spezieller Software, die Nutzung des Datenträger-Löschbefehls, sofern das Speichermedium dies unterstützt, oder das Verschlüsseln von Daten und das anschließende Löschen der Schlüssel. Letzteres schützt gegen unbefugte Wiederherstellung. Bei Smartphones und Tablets kann zudem ein Zurücksetzen auf die Werkseinstellungen erfolgen, wobei darauf geachtet werden muss, die Option zur vollständigen Inhaltslöschung zu wählen. In Fällen, wo eine Überschreibung nicht möglich ist, empfiehlt sich die physische Zerstörung des Speichermediums.

Unsichere Methoden und Empfehlungen

Allerdings gibt es auch zahlreiche unsichere Methoden zur

Datenlöschung. Die Löschung über den Papierkorb ist nicht ausreichend, da die Dateien weiterhin auf dem Medium existieren und wiederhergestellt werden können. Das Zurücksetzen auf die Werkseinstellungen löscht häufig nur die Struktur der Daten, nicht aber die Daten selbst. Ebenso garantiert eine einfache Formatierung keine vollständige Entfernung der Daten. Das BSI weist darauf hin, dass insbesondere schützenswerte persönliche Daten wie E-Mails, Fotos und Passwörter sicher gelöscht werden sollten, um einem ungewollten Zugriff entgegenzuwirken.

Insgesamt bleibt festzuhalten, dass ein bewusster Umgang mit Daten und deren Löschung essenziell ist. Ob beim Entsorgen von Geräten oder beim Sichern sensibler Informationen – die richtigen Maßnahmen bieten den nötigen Schutz. Die Empfehlung, vor der Löschung ein Backup der benötigten Daten zu erstellen, rundet die Hinweise des BSI ab. Umfassende Sicherheit kann nur gewährleistet werden, wenn die Löschmethoden mit Bedacht gewählt werden.

Weitere Informationen zu diesem Thema sind auf der Webseite des **BSI** zu finden.

Details	
Ort	Deutschland
Quellen	<ul style="list-style-type: none">• www.faz.net• www.bsi.bund.de

Besuchen Sie uns auf: n-ag.net