## 7. Schalten Sie aus, was Sie nicht brauchen

Funkverbindungen wie WLAN, Bluetooth, GPS oder NFC sind praktisch, bergen aber auch Risiken: Sie können von Dritten genutzt werden, um auf Ihre Geräte zuzugreifen oder Ihr Verhalten zu verfolgen. Schalten Sie solche Funktionen deshalb immer aus, wenn Sie sie nicht aktiv benötigen, insbesondere an öffentlichen Orten. So reduzieren Sie die Angriffsfläche für potenzielle Hacker und schonen zusätzlich den Akku Ihres Geräts.

Auch bei Apps lohnt sich ein Blick in die Einstellungen: Viele Anwendungen verlangen Zugriff auf Standort, Kamera oder Mikrofon, obwohl das für deren Funktion gar nicht notwendig ist. Prüfen und beschränken Sie solche Berechtigungen regelmäßig, um zu verhindern, dass Sie ausspioniert und Ihre persönlichen Daten missbraucht werden.

## 8. Schützen Sie Ihre Privatsphäre

In sozialen Netzwerken wie Facebook und Instagram geben viele Menschen persönliche Informationen preis – oft mehr, als ihnen bewusst ist. Achten Sie darauf, wer Ihre Beiträge sehen kann, und passen Sie die Privatsphäre-Einstellungen Ihrer Konten sorgfältig an. Vermeiden Sie es, sensible Daten wie Adresse, Telefonnummer oder Urlaubspläne öffentlich zu teilen.

Auch Ihr Browser bietet Einstellungen, mit denen Sie Ihre Privatsphäre schützen können, etwa durch Einschränkungen beim Setzen von Cookies oder die Aktivierung der „Do-Not-Track“-Funktion. Je weniger Spuren Sie im Netz hinterlassen, desto besser sind Sie vor Profilbildung und Datenmissbrauch geschützt.

## 9. Vorsicht bei Links und E-Mail-Anlagen

Links und Dateianhänge in E-Mails oder Nachrichten können gefährlich sein, auch wenn sie auf den ersten Blick harmlos wirken. Kriminelle tarnen ihre Schadsoftware häufig als scheinbar seriöse Nachricht, z. B. als Paketbenachrichtigung, Rechnung oder Gewinnspiel. Klicken Sie deshalb nie unbedacht auf Links und öffnen Sie nur Anhänge, die Sie selbst angefordert ober erwartet haben. Seien Sie besonders vorsichtig, wenn Ihnen ein unerwarteter Anhang von einer bekannten Adresse geschickt wird, denn Absenderadressen lassen sich leicht fälschen. Fragen Sie im Zweifel lieber beim Absender nach, aber nicht über die Kontaktdaten aus der Nachricht selbst, sondern über einen bekannten, sicheren Kanal. So vermeiden Sie, versehentlich Malware zu installieren oder auf gefälschte Webseiten hereinzufallen.

## 10. Vorsicht beim Onlinebanking

Onlinebanking ist bequem, erfordert aber besondere Vorsicht. Nutzen Sie nur sichere Verfahren, z. B. mit einem TAN-Generator oder einer offiziellen App Ihrer Bank. Geben Sie PINs, TANs oder Zugangsdaten niemals an Dritte weiter und speichern Sie sie nicht im Browser. Öffnen Sie keine Banking-Seite über Links in E-Mails oder SMS – diese könnten gefälscht sein. Rufen Sie Ihre Bank stets direkt über die bekannte Internetadresse oder die offizielle App auf. Zusätzlich kann es sinnvoll sein, ein Überweisungslimit einzurichten, um den möglichen Schaden im Ernstfall zu begrenzen.

## Bleiben Sie auf dem neuesten Stand

Die Erfahrung zeigt, dass sich die Methoden der Kriminellen immer weiterentwickeln. Deshalb ist es uns wichtig, Sie stets über neue Gefahren aber auch Gegenmaßnahmen zu informieren. Auf unserer Homepage finden Sie laufend aktualisierte Hinweise und Tipps, um sich und Ihre Finanzen zu schützen. Dringende Warnhinweise veröffentlichen wir auch unverzüglich über unsere Social Media Kanäle.

**vr-memmingen.de/sicherheit**

VR-Bank
Memmingen eG
Maximilianstraße 24 · 87700 Memmingen

# Sicher unterwegs im Internet

10 Gebote für mehr Cyber Security

# Tatort www

VR-Bank
Memmingen eG

VR-Bank Memmingen eG

# 10 Gebote für mehr Cyber Security

## 1. Bilden Sie sich weiter

Wer sich sicher im Straßenverkehr bewegen will, benötigt nicht nur ein zuverlässiges Fahrzeug, sondern muss auch Gefahrensituationen rechtzeitig erkennen und richtig reagieren, um Schäden zu vermeiden. Ganz ähnlich ist es mit dem Internet. Aber keine Sorge. Sie müssen nicht gleich zum IT-Experten werden. Es genügt, sich mit den Grundlagen der Computerbenutzung auseinanderzusetzen, um sich sicher im Internet zu bewegen.

Hilfreiche Informationen finden Sie z. B. unter bsi.bund.de, verbraucherzentrale.de oder sicher-im-netz.de

## 2. Sichern Sie Ihre Geräte

Egal ob Windows-PC, Mac, Smartphone oder Tablet – alle Geräte, mit denen Sie ins Internet gehen, sollten gut geschützt sein. Verwenden Sie auf Ihrem Computer eine zuverlässige Sicherheitslösung: Betriebssysteme wie Windows enthalten bereits integrierte Schutzprogramme wie den Microsoft Defender, die in der Regel ausreichend sind, wenn sie aktuell gehalten werden.

Richten Sie für Mobilgeräte unbedingt einen sicheren Zugriffsschutz ein (PIN, Fingerabdruck oder Gesichtserkennung) und aktivieren Sie die automatische Gerätesperre. Laden Sie Apps ausschließlich aus offiziellen App-Stores (z. B. Google Play oder Apple App Store) herunter, wo sie auf Schadsoftware geprüft wurden.

Zusätzlich hilft eine Firewall, wie sie in vielen Betriebssystemen bereits enthalten ist, um unerwünschten Datenverkehr zu blockieren und Ihr Netzwerk abzusichern. Achten Sie darauf, alle Sicherheitsfunktionen regelmäßig zu prüfen und zu aktivieren, damit Sie im Alltag zuverlässig vor Angriffen geschützt sind.

## 3. Halten Sie Ihre Software aktuell

Veraltete Programme enthalten oftmals Sicherheitslücken, die von Kriminellen gezielt ausgenutzt werden. Updates (auch „Patches“ genannt) schließen solche Lücken und verbessern zusätzlich die Stabilität und Leistung Ihrer Geräte. Das betrifft nicht nur das Betriebssystem (z. B. Windows, macOS, Android oder iOS), sondern auch Programme wie Webbrowser, Office-Anwendungen, E-Mail-Programme oder Sicherheitssoftware. Aktivieren Sie nach Möglichkeit die automatische Update-Funktion, damit wichtige Aktualisierungen im Hintergrund installiert werden, ohne dass Sie daran denken müssen.

Auch Geräte wie WLAN-Router, vernetzte Haushaltsgeräte (Smart Home) oder Smart-TVs sollten regelmäßig aktualisiert werden. Wenn diese Geräte keine automatischen Updates unterstützen oder der Hersteller keine Sicherheitsaktualisierungen mehr bereitstellt, sollten Sie einen Austausch in Erwägung ziehen.

Wichtig: Installieren Sie Updates nur aus vertrauenswürdigen Quellen und klicken Sie niemals auf Update-Meldungen, die Ihnen per E-Mail oder Pop-up-Fenster im Browser angezeigt werden. Dabei handelt es sich oft um betrügerische Fälschungen.

## 4. Schützen Sie Ihre Benutzerkonten

Um Ihre Online-Konten und damit sensible Daten zuverlässig vor Missbrauch zu schützen, ist ein sicheres Passwort allein oft nicht mehr ausreichend – aber es ist der wichtigste erste Schritt. Ein sicheres Passwort besteht aus mindestens 14 Zeichen und enthält Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen. Vermeiden Sie echte Wörter, Namen oder Geburtsdaten. Verwenden Sie unbedingt für jeden Dienst ein eigenes Passwort. Wird ein Konto gehackt, bleiben somit alle anderen weiterhin geschützt. Da es schwierig sein kann, sich viele komplexe Passwörter zu merken, lohnt sich die Nutzung eines Passwortmanagers wie Bitwarden, 1Password oder KeePass.

Wo immer möglich, sollten Sie zusätzlich die Zwei-Faktor-Authentifizierung (2FA) aktivieren. Damit geben Sie neben dem Passwort z. B. noch einen Code ein, der an Ihr Smartphone geschickt oder über eine App generiert wird. Selbst wenn Kriminelle Ihr Passwort dann herausfinden, kommen sie ohne den zweiten Faktor nicht in Ihr Konto.

## 5. Surfen Sie nicht als Admin

Ein Admin-Konto (kurz für „Administrator“) hat viel mehr Rechte als ein herkömmliches Benutzerkonto: Darüber können Programme installiert, Systemdateien geändert oder Sicherheitsfunktionen abgeschaltet werden. Genau das macht es so gefährlich, wenn Schadsoftware aktiv wird, während Sie als Admin angemeldet sind. Denn sie erhält dieselben Rechte wie das aktuell aktive Benutzerkonto. Viren oder Trojaner können damit deutlich größeren Schaden anrichten, etwa wichtige Dateien verändern, neue Programme installieren oder das System komplett übernehmen.

Erstellen Sie deshalb ein zusätzliches Benutzerkonto mit eingeschränkten Rechten für das alltägliche Surfen und Arbeiten. Nur wenn Sie Software installieren oder Systemeinstellungen ändern wollen, melden Sie sich gezielt mit dem Admin-Konto an. Wenn mehrere Personen denselben Computer nutzen – etwa in Familien –, sollte jeder ein eigenes Konto mit individuellen Berechtigungen erhalten. Auf mobilen Geräten gibt es meist keine klassische Trennung zwischen Admin- und Standardkonten.

## 6. Vorsicht beim Surfen

Kriminelle versuchen mit gefälschten Webseiten und E-Mails an Ihre Zugangsdaten zu gelangen oder Schadsoftware auf Ihrem Gerät zu installieren. Seien Sie deshalb beim Surfen stets aufmerksam. Achten Sie darauf, dass Webseiten mit https:// (und nicht bloß mit http://) beginnen und – je nach Browser– ein Schloss-Symbol in der Adresszeile des Browsers angezeigt wird, was auf eine gesicherte Verbindung hindeutet. Klicken Sie niemals unüberlegt auf Links oder Pop-ups und laden Sie keine Dateien von unbekannten Quellen herunter. Halten Sie Ihren Browser stets aktuell, um Sicherheitslücken zu schließen. Wenn Sie möchten, können Sie zusätzlich Erweiterungen wie Werbeblocker oder Anti-Tracking-Tools installieren, die das Surfen sicherer machen. Vertrauen Sie auf Ihr Bauchgefühl: Wenn eine Seite merkwürdig aussieht, schließen Sie sie lieber sofort.