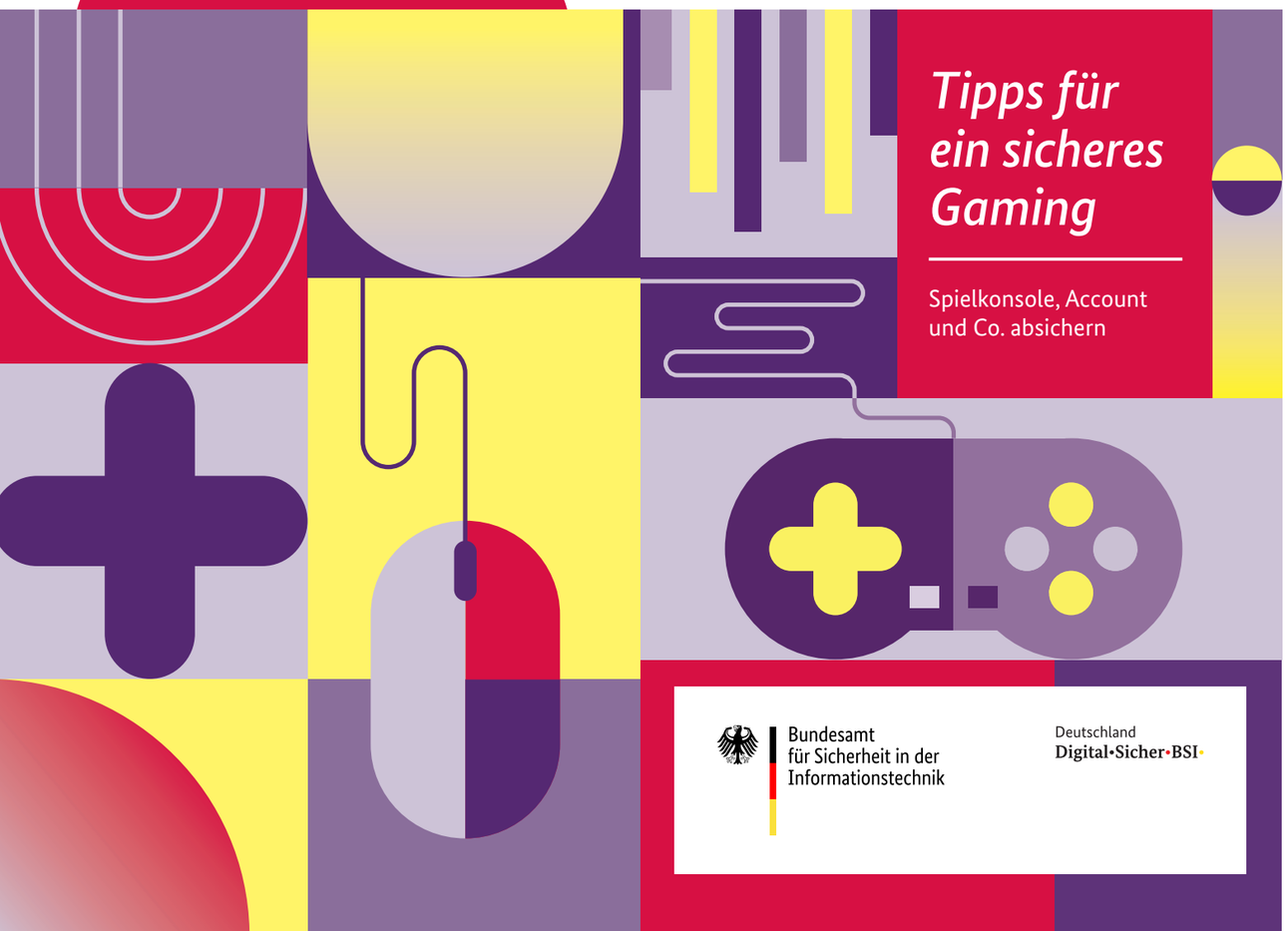
IT-Basisschutz fürs Gaming

Gamerinnen und Gamer tauchen in Video- und Online-Spielen in fantasievolle Welten und action-geladenes Gameplay ab. Für ihre Sicherheitseinstellungen nehmen sich viele jedoch kaum Zeit und ein Hack des Gaming-Accounts oder der Missbrauch der hinterlegten Kreditkarte wird zum absoluten Endgegner.

Wir sagen: Schon wenige Minuten reichen, um die Konsole, das Handy oder den Gaming-PC bereits VOR dem Gaming-Erlebnis gut abzusichern.



Gaming – 8 Spielregeln für eure digitale Sicherheit

Wer seine Spielekonsole, den PC oder das mobile Gerät für Video- und Online-Spiele nutzt, sollte sich vor dem Gaming-Erlebnis einen Moment Zeit für die digitale Sicherheit nehmen. Mit den folgenden Tipps steht dem nächsten Gaming-Marathon nichts im Wege.

1. Accounts mit mehreren Faktoren absichern
2. Games nur aus sicheren Quellen herunterladen
3. Starke Passwörter vergeben
4. Vorsicht bei Account-Sharing
5. Käufe von In-Game-Items überprüfen
6. Separates Benutzerkonto einrichten
7. Regelmäßige Updates installieren
8. Datenschutz- und Privatsphäreeinstellungen überprüfen

Schon gewusst?

Schon vor dem Zocken an die Sicherheit denken

Wer kennt es nicht? Das neue Spiel ist gerade eben heruntergeladen oder die neue Konsole frisch ausgepackt – man will sofort loszocken und keine Zeit verlieren! Doch um keine bösen Überraschungen zu erleben, ist es elementar wichtig, sich vor dem Zocken ein paar Minuten Zeit für die eigene digitale Sicherheit zu nehmen!

Insbesondere die Gaming-Accounts sind dabei von zentraler Bedeutung. Wir brauchen sie, um Hard- und Software zu kaufen, um Spiele herunterzuladen, online zu spielen oder um Updates zu installieren. Das bedeutet, über eine lange Gamer-Karriere sammeln sich viele Accounts und Konten an, die sich u.a. mit persönlichen Informationen und Zahlungsdaten füllen. Kapern Kriminelle das Nutzerkonto, können sie damit auf virtuelle Shopping-Tour gehen oder Loot erbeuten. Manche verwenden die Daten aber auch, um Straftaten zu begehen und nutzen beispielsweise fremde Identitäten, um zu stehlen und zu betrügen. Um sich gegen Phishing zu schützen, sollten z.B. Rabattaktionen auf Echtheit geprüft und generell besonderen Wert auf Datensparsamkeit gelegt werden.

Weitere Informationen

Digitaler Verbraucherschutz: Sicherer Umgang mit Informationstechnik

Sicherheit beim Gaming

Schritt für Schritt zur Zwei-Faktor-Authentisierung für Gaming-Accounts

Impressum

Herausgeber:
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 185-189, 53175 Bonn

Kontakt:
E-Mail: service-center@bsi.bund.de
Internet: www.bsi.bund.de
Service-Center: +49 (0) 800 274 1000

Artikelnummer:
BSI-IFB 23/151

1. Accounts mit mehreren Faktoren absichern

Um schnell ins Game einzusteigen, wird oftmals nur der Benutzername (oder Online-ID) sowie ein Passwort verlangt. Da gleichzeitig aber auch einige sensible Informationen wie z.B. Zahlungsdaten hinterlegt werden müssen, um das Spiel zu starten, sollte der Gaming-Account mit der Zwei-oder Mehr-Faktor-Authentisierung abgesichert sein.

Wie der Name schon sagt, fügt man dem bestehenden Anmeldeverfahren in diesem Fall eine oder mehrere Sicherheitsebenen hinzu. Diese **mehrstufige Authentisierung** ist auf der Konsole in den Einstellungen in der Konto-Verwaltung zu finden. Eine Authentisierung mittels mehrerer Faktoren beginnt in vielen Fällen mit der gewöhnlichen Eingabe eines **starken Passworts**. Faktor zwei kann dann ein **Fingerabdruck, ein Code per E-Mail oder SMS**, aber auch ein **TAN-Generator** sein. Man besitzt also gewissermaßen ein einmaliges Item, das den Gaming-Account zusätzlich schützt.

2. Games nur aus sicheren Quellen herunterladen.

Software, die heruntergeladen wird, kann Schadcode enthalten. Ist dieser einmal – meist unbemerkt - auf einem Gerät, ist weiterer Schaden kaum abwendbar. Ist der Ursprung eines Games unbekannt oder stammt es aus einem illegalen Download, sollte man von der Installation absehen.

Indizien für eine unseriöse Quelle können ein konkurrenzlos günstiger Preis oder ein fehlendes Impressum sein. Spiele sollte man also nur aus offiziellen Quellen herunterladen. Dazu zählen die Stores der Smartphone-Hersteller oder die großen Software-Shops, die mit den Entwicklern und Entwicklerinnen zusammenarbeiten.

3. Starke Passwörter vergeben

Hacker können vollautomatisch alle möglichen Zeichenkombinationen ausprobieren, ganze Wörterbücher einschließlich gängiger Wort-Zahl-Kombinationen testen oder einmal im Internet veröffentlichte Zugangsdaten bei allen möglichen Diensten durchprobieren. Es muss also ein starkes Passwort her!

Neben der Zwei- oder Mehr-Fak tor-Authentisierung ist es wichtig, für jeden Account ein **individuelles Passwort** zu erstellen. Dieses Passwort kann entweder relativ kurz (mindestens acht Zeichen), aber dafür komplex sein oder aber es ist deutlich länger und enthält weniger unterschiedliche Zeichenarten. Damit man sich nicht jedes Passwort merken muss, empfiehlt es sich, einen **Passwort-Manager** zu verwenden, der starke Passwörter für jeden Dienst erstellt. So muss man sich nur das **Masterpasswort** des Passwort-Managers merken.

4. Vorsicht bei Account-Sharing

Account-Sharing sollte gut überlegt sein, denn sind die eigenen Zugangsdaten einmal mit Freunden und Bekannten geteilt, könnte der Account (un)beabsichtigt in die falschen Hände gelangen und finanzieller Schaden entstehen. Außerdem gibt es Konsolen bzw. Anbieter, die Account-Sharing verbieten.

Das BSI **rät vom Account-Sharing ab**. Falls man den Account unter gewissen Umständen trotzdem teilen möchte, dann sollten die Zugangsdaten nur an Personen gelangen, denen man **wirklich vertraut**. Außerdem ist es sinnvoll, **automatische Nachrichten** zu aktivieren, wenn sich jemand Neues im Account einloggt.

5. Käufe von In-Game-Items überprüfen

Viele Games bieten Items an, die nicht im ursprünglichen Kaufpreis enthalten sind oder die einen schnelleren Spielfortschritt versprechen. Es kann passieren, dass man so in eine Kostenfalle gelockt wird oder bei einem Fremdzugriff auf den eigenen Account weitere hohe Kosten entstehen.

Damit man für seinen Geldbeutel eine zusätzliche Hürde einbaut und vor allem nicht versehentlich in eine **Kostenfalle** tappt, sollten In-App-Käufe passwortgeschützt sein. Damit vermeidet man, mit nur einem Klick bzw. **unbeabsichtigt Käufe** zu tätigen. Außerdem sollten die **Zahlungsdaten nicht dauerhaft hinterlegt** sein, sondern nur bei Bedarf eingegeben werden. Die Zahlungsmethode sollte durch einen **zusätzlichen Faktor** (s. Punkt 1) abgesichert sein, um im Falle einer Fremdübernahme des Accounts einen Missbrauch zu erschweren.

6. Separates Benutzerkonto einrichten

Administrator-Benutzerkonten erlauben Eingriff in die tiefsten Strukturen eines Systems. Im Falle eines Hacks oder beim Befall von Schadsoftware laufen sie Gefahr, von tiefgreifenden Manipulationen betroffen zu sein.

Empfehlenswert ist die **Einrichtung mehrerer Benutzerkonten** mit unterschiedlichen Rechte-Niveaus. Beim Gaming sollte man nur auf jenes Nutzerkonto des Rechners oder der Konsole zurückgreifen, das über eingeschränkte Rechte verfügt und auf dem **nur die nötigsten Daten** hinterlegt sind. Insbesondere bei Gaming-PCs sollte man ein separates Benutzerkonto mit **eingeschränkten Zugriffsrechten** einrichten.

7. Regelmäßige Updates installieren.

Sind die Geräte, der Gaming-PC oder die Konsole, nicht mit den aktuellsten Sicherheitsupdates versorgt, öffnet dies Kriminellen Tür und Tor.

Optimal wäre: Man aktiviert in den Einstellungen des PCs, Smartphones oder der Konsole die **automatischen Updates**. Denn grundsätzlich ist es ratsam, Hersteller-Updates nicht aufzuschieben und zunächst eine Runde zu zocken, sondern sie **schnellstmöglich herunterzuladen und zu installieren**, sobald sie verfügbar sind.

8. Datenschutz- und Privatsphäreeinstellungen überprüfen

Persönliche Daten zu teilen oder dauerhaft zu hinterlegen, erscheint manchmal reizvoll bzw. bequem. Doch sie können genutzt werden, um personifizierte Werbung zu generieren, Online-Verhalten nachzuvollziehen oder Identitäten zu kopieren.

Es kann sich lohnen, in der Konsole oder innerhalb des Games die Datenschutzeinstellungen zu überprüfen und nur absolut notwendige Datenübertragungen zuzulassen. Kreditkartendaten oder andere sensible Informationen sollten niemals preisgegeben werden, um kein Opfer von Phishing zu werden. Denn: Datensparsamkeit ist das erste Mittel, damit sensible Informationen nicht gestohlen und missbraucht werden können.