Vorsicht vor unseriösen Handwerkern! >
< Miese Masche

Betrug beim Online-Gaming

Cyber-Kriminelle haben unvorsichtige Spieler im Visier

Online-Spieler sind besonders anfällig für Betrüger

30 Millionen Deutsche spielen regelmäßig Computer- und Videospiele, wie eine repräsentative Umfrage im Auftrag des Digitalverbands Bitkom ergab. Bekannte Games wie „World of Warcraft“, „League of Legends“ oder „Candy Crush Saga“ sind populär. Spiele im Netz erfreuen sich wachsender Beliebtheit. Doch hinter Apps und Avataren lauern immer öfter auch Betrüger, die es auf das virtuelle Guthaben der Spieler abgesehen haben, deren Konten knacken wollen oder gefährliche Schadprogramme verbreiten.

Spieler im Visier von Hackern

Immer mehr Menschen spielen PC- und Videospiele im Netz. Sie kämpfen gemeinsam gegen Drachen oder liefern sich rasante Rennen mit virtuellen Sportwagen (Boliden). Wer in seiner Freizeit gerne Online-Games spielt, sollte sich gut vor Cyber-Kriminellen schützen. Nicht jede Mail oder Webseite muss seriös sein, auch wenn der Absender zunächst wie der Anbieter des erworbenen Spiels aussieht. Hinter Phishing-Mails und -Webseiten stecken häufig Kriminelle, die es auf Passwörter und Kreditkarteninformationen abgesehen haben. Online-Spieler, die sich zum Spielen mit anderen Menschen im Internet treffen, sind beliebte Opfer dieser Masche. Mit gefälschten Webseiten von beliebten Multiplayer-Spielen wollen die Betrüger unaufmerksame Nutzer hereinlegen. Wer hier bereitwillig sein Passwort eingibt, riskiert, dass sein Konto geknackt und auf dem Schwarzmarkt verkauft wird.

- Achten Sie auf Rechtschreibfehler in angeblich offiziellen Mitteilungen des Herstellers und fragen Sie

- im Zweifel beim Support nach.
- Mit einem erfolgreichen Avatar sollten Sie besonders auf Ihr Spieler-Konto achten.
- Richten Sie ein komplexes Passwort mit möglichst vielen Buchstaben und Zeichen für das Spieler-Konto und die damit verknüpfte E-Mail-Adresse ein.

Doch selbst solche Maßnahmen nützen kaum, wenn es Kriminelle auf den Anbieter abgesehen haben. Im Jahr 2011 gab der Großkonzern Sony bekannt, dass das Online-Netzwerk seiner aktuellen Spielekonsole gehackt wurde. Bei dem Angriff sind auch Kundendaten gestohlen worden. Da mittlerweile alle gängigen Heimkonsolen über einen Zugang ins Internet verfügen, haben es Cyber-Kriminelle auf die vielen Konsolenspieler abgesehen. Wer Kunde in einer solchen Community ist, sollte das eigene Bankkonto regelmäßig auf verdächtige Transaktionen überprüfen und die Zugangsdaten zum Spiele-Portal hin und wieder ändern. Sind Sie Kunde auf mehreren Plattformen, nutzen Sie für den Zugang niemals dasselbe Passwort. Die Daten von Gamern sind für Cyber-Kriminelle besonders wertvoll, da den Konten meist persönliche Fotos, Namen, Adressen und Standorte entnommen werden können. Haben Sie den Verdacht, dass Ihr Spieler-Konto einem Identitätsdiebstahl zum Opfer gefallen sein könnte, sollten Sie umgehend den Betreiber kontaktieren. Denn die Kriminellen können mit dem gekaperten Konto beispielsweise E-Mails verschicken, Beleidigungen posten und Ihr virtuelles Guthaben weiterverkaufen. Im Extremfall haben sie Zugriff auf die verknüpften Kreditkartendaten eines kostenpflichtigen Spieler-Kontos.

Bedrohungen lauern auch auf dem Smartphone

Neben PC und Konsole wird mittlerweile auch das Smartphone zum Spielen genutzt. Deshalb versuchen Betrüger über Apps an die Login-Daten zu kommen, um Bankkonten leerzuräumen oder das Smartphone mit einem Schadprogramm zu infizieren. Manchmal gelingt es den Kriminellen, gefälschte Apps mit Namen von bekannten Spielen im App Store, dem Marktplatz für mobile Spiele und Anwendungen, anzubieten. Dahinter verbergen sich zum Beispiel Trojaner, die stetig Werbung aufrufen. Mit jedem Klick eines Spielers auf eine Werbeanzeige verdienen die Betrüger Geld. Spieler sollten daher bei jeder kostenlos angebotenen App unbedingt die Kommentare von anderen Nutzern lesen, bevor sie die Anwendung herunterladen. Smartphones und die darauf installierten Programme müssen zudem mit regelmäßigen Updates vor Viren, Malware und Trojanern geschützt werden. Auch die Installation eines Anti-Viren-Programms bietet einen wirkungsvollen Schutz vor schwarzen Schafen. Solche Programme haben meist auch einen Modus, der sich beim Spielen nicht verlangsamend auf die Rechenkapazitäten des Handys auswirkt.

Kinder sind besonders gefährdet

Im Internet spielen vor allem Kinder und Jugendliche oft mit anderen Menschen, die sie im realen Leben nie getroffen haben. Eltern sollten ihre Kinder deshalb darauf hinweisen, dass sie unbekannten Mitspielern niemals ihre echte Identität oder persönliche Daten wie etwa den Wohnort mitteilen dürfen. Achten Sie auch darauf, dass Ihr Kind nicht auf Phishing-Versuche hereinfällt. Kinder können solche gefälschten Nachrichten schlechter als Fälschung enttarnen als Erwachsene. Deshalb versuchen die Cyber-Kriminellen, junge Nutzer mit vermeintlich kostenlosen Gimmicks und Spielen zu ködern. Bei der Nutzung von Spiele-Apps auf dem Smartphone sollten Kinder zudem keinen Zugriff auf sogenannte In-App-Käufe haben. Dahinter stecken zwar selten Betrüger, einige unseriöse Games locken aber mit aufdringlichen Angeboten und erlauben ein Weiterspielen erst beim Kauf teurer Extras. Hersteller von Anti-Viren-Programmen bieten auch Apps zur Kindersicherung auf dem Smartphone an, damit solche für die Eltern kostenpflichtigen Transaktionen in der Spiele-App ausbleiben. Dann steht dem Spielspaß beim Online-Gaming nichts mehr im Wege.

Eltern sollten ihre Kinder darauf hinweisen, dass sie unbekannten Mitspielern niemals ihre echte Identität preisgeben

AL (31.03.2017)

Folgende Artikel könnten Sie auch interessieren:

- Alle Fahrraddaten stets mobil dabei
- Fallen beim Geschenkekauf
- Schutz vor Cybermobbing
- Video: Internetkriminalität – So schütze ich mich!
- Schwarzarbeit sorgt für Milliardenschaden
- Gewinnspielbetrug am Telefon
- Cybercrime – Angriffe auf Unternehmen
- Romance Scamming – der Liebesbetrug
- Smartphones sind Wertsachen
- Spiele muss man spielen, um sie zu verstehen
- Mit Verboten kommt man nicht weit
- Die medialen Kinder
- Vom Smartphone bis zum Tablet-PC

Alle Artikel dieser Kategorie

Weitere Infos zum Thema Diebstahl / Betrug

Vertrauen ist gut, Kontrolle ist besser

Was tun bei unberechtigten Kontoabbuchungen?

Wer viel im Internet einkauft, kann bei seinen Zahlungen und...[mehr erfahren]

Mit dem Klemmbrett durch die Fußgängerzone

Betrügerische Spendensammler

Vor allem in den Sommermonaten, wenn sich viele Menschen in der...[mehr erfahren]

Gefälscht wird, was gefällt

Professionelle Kunstfälschungen

Kunstfälschungen sind für Laien nicht einfach zu erkennen. Und selbst...[mehr erfahren]

Buntmetalldiebstahl an Bahnanlagen geht zurück

Lebensgefährlicher Kabelklau

Hohe Metallpreise, kriminelle Energie und eine gehörige Portion...[mehr erfahren]

Wie viel Vertrauen gewähren, wie viel Kontrolle ausüben?

Diebstahl am Arbeitsplatz

Bei der Frage, ob ein Arbeitgeber seinen Angestellten vertrauen kann,...[mehr erfahren]
