

OUCH!

IN DIESER AUSGABE...

- Schützen Sie sich
- Schützen Sie Ihren Computer
- Wissenswertes für Eltern

Sicheres Online-Gaming

Überblick

Onlinespiele sind ein sehr unterhaltsamer Zeitvertreib, bergen jedoch auch ihre ganz eigenen Risiken. In diesem Newsletter besprechen wir, was Sie und Ihre Familie zu ihrem Schutz bei Onlinespielen unternehmen können.

Schützen Sie sich

Was Onlinespiele so unterhaltsam macht ist die Möglichkeit, mit Spielern auf der ganzen Welt zu kommunizieren und mit ihnen zu spielen oder gegen sie anzutreten. Häufig wissen Sie gar nicht, wer ihre Mitspieler überhaupt sind. Während der Großteil der Spieler einfach nur Spaß sucht, gibt es doch einige die Ihnen Schaden zufügen wollen. Hier sind einige Schritte die Sie zu Ihrem Schutz unternehmen können.

Gastautor

Steve Armstrong ist Gründer von Logically Secure, zertifizierter SANS Trainer, und Architekt von CyberCPR, einer Vorfallesverwaltungsplattform. Er ist auf Twitter als [@Nebulator](#) aktiv und arbeitet mit vielen großen Spielefirmen weltweit, um sich seine beruflichen, aber auch seine Kindheitsträume zu erfüllen.

Sie gar nicht, wer ihre Mitspieler überhaupt sind. Während der Großteil der Spieler einfach nur Spaß sucht, gibt es doch einige die Ihnen Schaden zufügen wollen. Hier sind einige Schritte die Sie zu Ihrem Schutz unternehmen können.

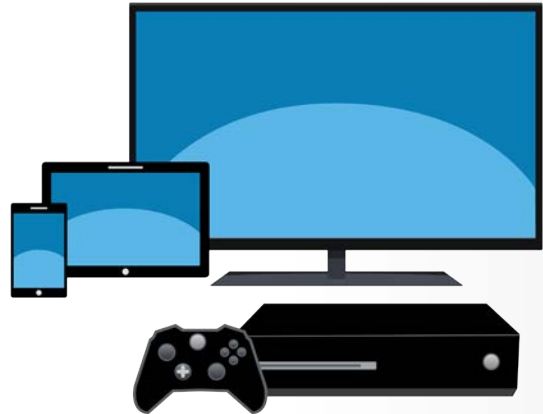
- Vorsicht bei allen Nachrichten, die von Ihnen eine Aktion anfordern, wie z.B. das Klicken eines Links oder das Herunterladen einer Datei. Genau wie Phishing-Angriffe per E-Mail werden Kriminelle versuchen, Sie zu Aktionen zu verleiten die zur Infektion Ihres Computers oder dem Diebstahl Ihrer Online-Identität dienen. Wenn eine Nachricht ungewöhnlich, eilig, oder zu gut um wahr zu sein erscheint, seien Sie auf der Hut!
- Viele Onlinespiele haben ihre eigenen Marktplätze, auf denen Sie handeln, tauschen oder sogar virtuelle Waren kaufen können. Genau wie in der echten Welt gibt es auch hier Betrüger, die versuchen Sie auszutricksen um an Ihr Geld oder die jeweilige virtuelle Währung zu gelangen. Handeln Sie nur mit Personen, die eine etablierte, vertrauenswürdige Reputation vorweisen können.
- Nutzen Sie auch für Ihre Spielekonten starke Passwörter. So können Angreifer Ihr Passwort nicht einfach erraten und damit Ihr Konto übernehmen. Wenn Ihr Spiel eine 2-Faktor-Anmeldung anbietet, nutzen Sie sie. Stellen Sie zudem sicher, dass all Ihre Onlinekonten über ein eigenes, individuelles Passwort verfügen. Wenn eines Ihrer Konten kompromittiert wird, sind die anderen somit noch sicher. Sie können sich all diese Passwörter nicht merken? Versuchen Sie es mit einem Passwortverwaltungsprogramm.

Schutz Ihres Systems

Kriminelle versuchen möglicherweise, den Computer an dem Sie spielen zu hacken oder zu übernehmen. Sie müssen daher Schritte unternehmen, ihn zu schützen.

Sicheres Online-Gaming

- Nutzen Sie immer die neueste Version Ihres Betriebssystems und halten Sie auch das Spiel selbst aktuell. Alte Software hat oft bekannte Schwachstellen, die Angreifer ausnutzen können um Ihren Computer anzugreifen. Indem Sie den Computer und die Spiele aktuell halten, eliminieren Sie die meisten dieser Schwachstellen.
- Nutzen Sie eine Virenschutzsoftware, stellen Sie sicher, dass diese aktuell ist, und dass sie alle Dateien in Echtzeit überprüft.
- Laden Sie Spielesoftware nur von vertrauenswürdigen Webseiten herunter. Häufig erstellen Cyberkriminelle schlecht nachgemachte oder infizierte Versionen von Spielen und verteilen sie dann über eigene Server.
- Erweiterungen, oft von der Spielergemeinschaft entwickelt, werden meist genutzt um neue Möglichkeiten ins Spiel einzubauen. Angreifer infizieren manchmal auch diese Erweiterungen mit Schadsoftware. Genau wie die Spiele selbst sollten daher auch Erweiterungen von vertrauenswürdigen Quellen geladen werden. Wenn eine Erweiterung das Deaktivieren Ihres Virenschutzes oder Änderungen an Ihren Sicherheitseinstellungen erfordert, sehen Sie von dieser Erweiterung ab.
- Um Betrugereien bei Onlinespielen zu unterstützen, haben sich ganze Untergrundmärkte entwickelt. Abgesehen davon, dass es sich dabei um unethisches Verhalten handelt, sind manche Cheatingprogramme selbst Schadsoftware, die Ihren Computer infizieren wird. Nutzen Sie nie irgendeine Form von Cheatingsoftware oder besuchen Sie derartige Webseiten.
- Besuchen Sie die Webseiten des Spiels, das Sie spielen. Oft finden Sie hier Informationen wie Sie sich selbst und Ihr System schützen können.
- Auch auf Ihren Mobilgeräten gilt, was für den Schutz Ihres Computers gilt. Cyberkriminelle haben auch diese Geräte bereits im Visier.



Wichtig für sicheres Onlinespielen sind starke Passwörter, ein abgesicherter Computer und eine gute Portion gesunder Menschenverstand, wenn Sie Nachrichten oder Anforderungen erhalten.

Wissenswertes für Eltern

Kinder benötigen eine Extraportion Schutz und Aufklärung hinsichtlich Onlinespielen. Ein offenes Gespräch und das damit vermittelte Wissen ist oft der beste Schutz für Kinder. Einer unserer besten Tricks, um mit Kindern ein solches Gespräch zu führen, ist sie zu bitten Ihnen ihr Lieblingsspiel zu erklären, sich ihre Onlinewelt zeigen zu lassen und sie bei einem typisches Spiel einfach mal zu begleiten, ja vielleicht sogar mitzuspielen. Lassen Sie sich von ihnen zudem die verschiedenen Personen beschreiben, mit denen sie online interagieren. Onlinespiele stellen oft einen beträchtlichen Teil

Sicheres Online-Gaming

des Soziallebens Ihrer Kinder dar. Indem Sie mit ihnen sprechen und ein offenes Ohr für sie haben, können Sie Probleme erkennen und sie viel besser schützen als mit jeder Technologie. Was können Sie noch tun?

- Stellen Sie sicher, dass Sie wissen welche Spiele die Kinder spielen und dass die Spiele altersgerecht sind.
- Begrenzen Sie die Menge der Daten, die Ihre Kinder online teilen. Sie sollten z.B. nie ihr Passwort, Alter, ihre Telefonnummer oder Adresse angeben.
- Stellen Sie den Spielecomputer wenn möglich, an eine zentrale Stelle der Wohnung, so dass Sie leicht einen Blick darauf werfen können. Gerade jüngere Kinder sollten nicht allein in ihren Zimmern und nicht spätabends in Onlinespielen unterwegs sein.
- Gemeinheiten gegenüber Anderen und ein schlechter Umgangston können zum Problem werden. Achten Sie auf die Reaktionen Ihrer Kinder, wenn sie nach einem Spiel aufgeregt oder betrübt sind, wurden sie vielleicht gemobbt. Sollte das der Fall sein, unterbinden Sie die weitere Teilnahme an dem Spiel und sorgen Sie dafür, dass Ihr Kind seine Zeit mit kindgerechteren Spielen verbringt oder mit solchen, die es nur gegen bekannte Freunde spielt.
- Prüfen Sie, ob die Spiele Ihrer Kinder Einkaufsmöglichkeiten beinhalten, und welche Möglichkeiten der elterlichen Einflussnahme es diesbezüglich gibt.

Weiterführende Informationen

Absicherung Ihres Heimnetzwerks:

<https://securingthehuman.sans.org/ouch/2016#february2016>

Social Engineering:

<https://securingthehuman.sans.org/ouch/2017#january2017>

Passphrasen:

<https://securingthehuman.sans.org/ouch/2017#april2017>

Password Manager:

<https://securingthehuman.sans.org/ouch/2015#october2015>

2-Faktor-Authentifizierung:

<https://securingthehuman.sans.org/ouch/2015#september2015>

Informieren Sie Sich

Abonnieren Sie den monatlichen OUCH! Security Awareness Newsletter, greifen Sie auf die OUCH! Archive zu und lernen Sie mehr über SANS Security Awareness Angebote unter securingthehuman.sans.org/ouch/archives.

Deutsche Ausgabe

Diese OUCH! Ausgabe wurde von Marek Kreul und René Wiedewilt aus dem Englischen übersetzt. Beide arbeiten für das CERT eines DAX-Konzerns und haben sich auf IT-Forensik spezialisiert. Sie haben langjährige Erfahrung im Bereich IT-Sicherheit und sind mehrfach GIAC zertifiziert.

OUCH! wird durch das SANS Securing The Human Programm herausgegeben und unter der [Creative Commons BY-NC-ND 4.0 Lizenz](https://creativecommons.org/licenses/by-nc-nd/4.0/) vertrieben. Die Erlaubnis zur Weitergabe dieses Newsletters oder Verwendung in einem Weiterbildungsprogramm wird gewährt, solange der Newsletter unverändert bleibt. Für Übersetzungen und weitere Informationen kontaktieren Sie bitte ouch@securingthehuman.org.

Redaktionsleitung: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley



securingthehuman.sans.org/blog



[/securethehuman](https://securethehuman)



[@securethehuman](https://twitter.com/securethehuman)



securingthehuman.sans.org/gplus