SANS SECURITY AWARENESS

Der monatliche Security Awareness Newsletter für Sie

Sicher online einkaufen

Übersicht

Die Weihnachtszeit nähert sich für viele von uns und bald werden Millionen von Menschen versuchen, die perfekten Geschenke zu kaufen. Viele von uns werden online einkaufen, um nach günstigen Angeboten zu suchen und Menschenmassen zu meiden. Leider werden auch Cyberkriminelle aktiv sein, die gefälschte Shopping-Webseiten erstellen und andere Taktiken anwenden, um Menschen zu betrügen. In diesem Newsletter erfahren Sie, wie Sie sicher im Internet einkaufen und nicht zum Opfer werden.

Gefälschte Online-Shops

Cyberkriminelle erstellen gefälschte Online-Shops, die das Aussehen echter Webseiten nachahmen oder die Namen bekannter Shops oder Marken verwenden. Wenn Sie nach den besten Online-Angeboten suchen, können Sie sich auf einer dieser gefälschten Seiten wiederfinden. Durch den Einkauf über solche Webseiten können Sie gefälschte oder gestohlene Gegenstände erwerben und in einigen Fällen werden Ihre Einkäufe möglicherweise nie zugestellt. Mit den folgenden Schritten schützen Sie sich vor gefälschten Online-Shops:

Kaufen Sie, wenn möglich, in Online-Shops, die Sie bereits kennen, denen Sie vertrauen und mit denen Sie bereits Geschäfte gemacht haben. Setzen Sie sich Lesezeichen für Online-Shops, die Sie schon einmal besucht haben und denen Sie vertrauen.

Achten Sie auf Preise, die deutlich besser sind als die, die Sie in den etablierten Online-Shops sehen. Wenn das Angebot zu gut klingt, um wahr zu sein, kann es gefälscht sein.

Seien Sie misstrauisch, wenn die Webseite derjenigen ähnelt, die Sie in der Vergangenheit benutzt haben, aber der Domänenname der Website oder der Name des Geschäfts ein anderer ist. So kann Sie ein unachtsames Klicken beispielsweise auf www.amaz0n.de führen - eine gefälschten Webseite mit einer ähnlichen Adresse wie das echte Amazon, wobei aber der Buchstabe o durch die Zahl 0 in der Adresse ersetzt wurde.

Geben Sie den Namen oder die Webadresse eines Online-Shops in eine Suchmaschine ein um zu sehen, was andere über ihn gesagt haben. Achten Sie auf Begriffe wie “Betrug”, “Schwindel” und “Fälschung”.

Nutzen Sie für jedes Konto ein individuelles Passwort. Sie können sich all diese Passwörter nicht merken? Dann ziehen Sie in Betracht, diese in einem Passwortmanager zu speichern.

Betrüger auf legitimen Webseiten

Schützen Sie sich auch beim Einkauf auf vertrauenswürdigen Webseiten. Große Online-Shops bieten oft Produkte an, die von verschiedenen Personen oder Unternehmen verkauft werden, die eventuell betrügerische Absichten haben könnten. Solche Online-Marktplätze sind wie reale Märkte, auf denen einige Verkäufer vertrauenswürdiger sind als andere. Überprüfen Sie den Ruf jedes Verkäufers, bevor Sie die Bestellung aufgeben. Achten Sie auf Verkäufer, die neu im Online-Shop sind oder Artikel zu ungewöhnlich niedrigen Preisen verkaufen. Überprüfen Sie die Richtlinien des Online-Shops für Einkäufe von Dritten. Kaufen Sie im Zweifelsfall Artikel, die direkt vom Betreiber des Online-Shops verkauft werden, und nicht über Drittanbieter, die auch über den Online-Shop anbieten.

Online-Zahlungen für Einkäufe

Überprüfen Sie regelmäßig Ihre Kreditkartenabrechnungen, um verdächtige Abbuchungen zu identifizieren. Wenn möglich aktivieren Sie die Option, sich per E-Mail, SMS oder App benachrichtigen zu lassen, wenn eine Belastung Ihrer Kreditkarte erfolgt. Wenn Sie verdächtige Aktivitäten feststellen, rufen Sie sofort Ihr Kreditkartenunternehmen an und melden Sie es. Verwenden Sie nach Möglichkeit keine Debitkarten. Debitkarten buchen das Geld direkt von Ihrem Bankkonto ab; wenn Sie betrogen wurden, haben Sie es viel schwerer, Ihr Geld zurückzubekommen. Eine weitere Möglichkeit ist die Nutzung bekannter Zahlungsdienste wie PayPal für Online-Einkäufe, bei denen Sie Ihre Kreditkartennummer nicht an den Verkäufer weitergeben müssen. Außerdem sollten Sie die Verwendung einer Gutscheinkarte für Online-Einkäufe in Betracht ziehen.

Nur weil ein Online-Shop ein gut gestaltetes, professionelles Aussehen hat, bedeutet das nicht, dass er legitim ist. Wenn Ihnen die Webseite ungewöhnlich erscheint, sollten Sie sie nicht benutzen. Besuchen Sie stattdessen eine bekannte Webseite, der Sie vertrauen können oder die Sie in der Vergangenheit sicher benutzt haben. Eventuell finden Sie das eine, unschlagbare, Angebot nicht, aber dafür werden Sie ein legales und seriöses Produkt erwerben und vermeiden, betrogen zu werden.

Gastredakteur

Lenny Zeltser *ist Chief Information Security Officer bei Axonius, und Senior Instructor und Autor am SANS Institute. Sie können ihm auf Twitter unter @lennyzeltser folgen und seinen Blog unter zeltser.com lesen.*

Weiterführende Informationen

Social Engineering:	http://www.sans.org/u/X7k
Betrügereien über Soziale Medien:	http://www.sans.org/u/X7p
Einfache Passwörter erzeugen:	http://www.sans.org/u/Xu9