Der monatliche Security Awareness Newsletter für Computeranwender

OUCH!

IN DIESER AUSGABE...

- Gefälschte Online Shops
- Ihr Computer / Mobilgerät
- Ihre Kreditkarte

Sicher Online Einkaufen

Die Saison der Vorsicht

Die Vorweihnachtszeit nähert sich und bald werden Millionen Menschen weltweit nach den perfekten Geschenken suchen. Viele davon werden auf der Suche nach einem Schnäppchen sein und zum Vermeiden von langen Warteschlangen Onlineshopping nutzen. Genau aus diesem Grund ist es auch die bevorzugte Zeit für Cyberkriminelle, um Online- oder Finanzbetrügereien zu begehen. Wir werden diese Ausgabe daher nutzen, um die Gefahren beim Onlineshopping zu erläutern und Ihnen Wege aufzuzeigen, wie Sie sich schützen können.

Gastautor

Jonathan Homer (**@JonathanLHomer**) ist im Bereich Cyber Security Awareness sehr bekannt und vermittelt sein Wissen sowohl im öffentlichen als auch im privaten Sektor. Jon hat sich darauf spezialisiert das Publikum in seine Schulungen aktiv einzubinden und nutzt darüberhinaus weitere innovative Schulungsstechniken.

Gefälschte Online Shops

Während es sich bei den meisten Onlineshops um legitime Seiten handelt, gibt es auch gefälschte Seiten die von Kriminellen betrieben werden. Sie kopieren dabei das Aussehen oder nutzen das Logo und den Schriftzug bekannter Webseiten. Dann versuchen Sie Menschen, die auf der Suche nach dem besten Preis sind, auf diese gefälschten Shops zu leiten. Wenn Sie online nach den absolut niedrigsten Preisen suchen, ist es leicht möglich, dass sie auf eine dieser gefälschten Seiten gelangen.
Achten Sie bei der Auswahl einer Webseite zum Kauf eines Produkts auf solche, deren Preis auffällig günstiger als bei anderen Mitbewerbern ist, oder auf Webseiten die Produkte anbieten die in den anderen Shops ausverkauft sind. Der Grund, warum diese Produkte so günstig bzw. überhaupt verfügbar sind liegt darin, dass Sie gefälschte, minderwertige oder gar gestohlene Ware erhalten - oder schlicht überhaupt nichts zugeschickt wird. Schützen Sie sich durch die folgenden Maßnahmen:

- Stellen Sie sicher, dass die Webseite eine legitime E-Mail Adresse und eine Telefonnummer für Beratung oder Hilfe besitzt. Wenn die Seite verdächtig aussieht, rufen Sie an und sprechen Sie mit einem Menschen.
- Achten Sie auf offensichtliche Warnhinweise wie schlechte Grammatik und Rechtschreibung.
- Seien Sie besonders vorsichtig, wenn eine Webseite wie eine genaue Kopie einer bekannten Webseite aussieht, die Sie in der Vergangenheit schon einmal besucht haben, gleichzeitig aber der Name der Seite oder des Shops leicht abweicht. Sie rufen gewöhnlich z.B. https://amazon.de auf, um bei Amazon einzukaufen. Eine ähnlich aussehende Webseite, die vorgibt Amazon zu sein aber die Adresse http://shop-amazon.de hat, ist äusserst verdächtig.

Sicher Online Einkaufen

- Tippen Sie den Namen oder die Webadresse des Shops in eine Suchmaschine um zu prüfen, was andere Nutzer darüber berichten. Suchen Sie nach Beiträgen die “Betrug”, “nie wieder” oder ähnliches enthalten. Das Fehlen von Bewertungen ist ein Hinweis, dass die Webseite sehr neu und damit vielleicht eine betrügerische Webseite ist.

Denken Sie daran, dass eine Webseite nicht legitim sein muss, nur weil sie professionell aussieht. Wenn auch nur ein einziges Merkmal der Webseite Ihre Alarmglocken schrillen lässt, prüfen Sie diesen Fakt genau. Wenn Sie sich nicht sicher sind, nutzen Sie diesen Shop besser nicht. Gehen Sie stattdessen auf eine bekannte Webseite mit guter Reputation, die Sie vielleicht sogar schon früher genutzt haben. Hier finden Sie womöglich kein ganz so gutes Angebot oder gar den überall ausverkauften Artikel, aber dafür bekommen Sie am Ende wenigstens das, wofür sie bezahlen.

Schützen Sie sich, indem Sie nur auf vertrauenswürdigen Webseiten und solchen mit einer guten Reputation einkaufen.

Ihr Computer / Mobilgerät

Zusätzlich zum Einkauf auf renommierten Webseiten sollten Sie auch darauf achten, dass das bei der Einkaufstour genutzte Gerät sicher ist. Die Angreifer werden versuchen, die Geräte zu infizieren, so dass sie Ihre Kontozugangsdaten, Kreditkarteninformationen und Passwörter stehlen können. Die folgenden Schritte helfen Ihnen bei der Absicherung Ihrer Geräte:

- Wenn Sie Kinder im Haus haben, überlegen Sie sich zwei separate Geräte anzuschaffen, eines für die Kinder und eines für die Eltern. Kinder sind neugierig und nutzen die Geräte ohne jegliche Scheu, wodurch sie ihr Gerät leider mit einer höheren Wahrscheinlichkeit infizieren. Durch die Nutzung eines separaten Geräts ausschließlich für Onlinetransaktionen wie Onlinebanking und Onlineshopping reduzieren Sie die Gefahr, dass dieses Gerät infiziert wird. Wenn separate Geräte keine Option sind, richten Sie zumindest getrennte Benutzerkonten auf Ihrem Computer ein, und stellen Sie sicher, dass Ihre Kinder nicht über administrative Berechtigungen verfügen.
- Verbinden Sie sich nur zu Drahtlosnetzwerken, die Sie selbst verwalten, wie z.B. Ihrem Heimnetz, oder Netzen von denen Sie wissen, dass Sie ihnen trauen können, wenn Sie Onlinetransaktionen durchführen wollen. Die Nutzung öffentlicher WLANs im lokalen Café mag zum Lesen der Zeitung toll sein, nicht jedoch für Ihre Bankgeschäfte.
- Installieren Sie immer die neuesten Updates für die von Ihnen genutzten Programme und lassen Sie die Antivirussoftware das Gerät regelmäßig überprüfen. Das macht es für Cyberkriminelle viel schwieriger, Ihr Gerät zu infizieren und dauerhaft zu kontrollieren.

Sicher Online Einkaufen

Ihre Kreditkarte

Prüfen Sie Ihre Kreditkartenabrechnungen, am besten regelmäßig einmal im Monat, um verdächtige Transaktionen zu finden. Einige Kreditkartenanbieter stellen sogar Funktionen bereit, um Sie bei jeder Belastung per E-Mail oder SMS zu informieren oder wenn Belastungen einen bestimmten Betrag überschreiten. Eine weitere Möglichkeit ist die Nutzung einer separaten Kreditkarte ausschließlich für Onlinetransaktionen. Diese kann leicht gewechselt werden, wenn sie missbraucht wird, ohne andere Abrechnungen in Mitleidenschaft zu ziehen. Wenn Sie eine betrügerische Transaktion vermuten, rufen Sie Ihr Kreditkartenunternehmen schnellstmöglich an und erläutern Sie die Situation. Aus genau diesem Grund sind Kreditkarten besser als z.B. EC-Karten oder Onlineüberweisungen. Bei der Nutzung von EC-Karten oder Onlineüberweisungen wird das Geld sofort transferiert und im Falle eines Betrugs erschwert dieser Fakt Ihrer Bank die Rückholung Ihres Geldes.

Ganz neu sind Verfahren, die es Ihnen ermöglichen Zahlungen zu leisten ohne Ihre Kreditkarteninformationen angeben zu müssen. Ziehen Sie derartige Kreditkarten in Betracht, die eine einzigartige Kreditkartennummer für jeden Onlineeinkauf generieren, oder nutzen Sie renommierte Bezahldienste wie Paypal, die eine Weitergabe Ihrer Bezahlinformationen an den Verkäufer unnötig machen.

Weiterführende Informationen

Sicher in fünf Schritten:	https://www.securingthehuman.org/ouch/2014#october2014
So sichern Sie Ihr Heimnetzwerk:	https://www.securingthehuman.org/ouch/2014#january2014
Absicherung Ihres neuen Tablet-Computers:	https://www.securingthehuman.org/ouch/2013#december2013
SANS Sicherheitstip des Tages (engl.):	https://www.sans.org/tip_of_the_day.php

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 http://www.securingthehuman.org.

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.

Redaktionsleitung: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis