Wie Sie sich selbst vor Phishing schützen: Empfehlungen von LeaderTelecom

Jeder kann Opfer von Internetbetrug werden. Sei es bei der Nutzung des Onlinebankings, bei Direktzahlungen über das Internet oder beim Online-Shopping mit Kreditkarte – schützen Sie sich mit diesen einfachen Tipps vor Internetbetrug.

Phishing: So fallen Sie nicht darauf herein

Eine Art des Internetbetrugs ist das Phishing. Dabei erspähen Hacker vertrauliche Daten, wie zum Beispiel Nutzernamen und Passwörter, oder Adressen und Kreditkartennummern. Sie gelangen normalerweise an diese Daten, indem Sie gefälschte Internetseiten erstellen, die dem Original sehr ähnlich sehen. Indem die Nutzer dann ihre echten Daten in die gefälschten Seiten eingeben, übermitteln sie den Betrügern unbewusst sämtliche persönlichen Informationen.

Kürzlich berichtete uns ein Nutzer des Bezahldienstes Paypal, wie er Opfer eines solchen Betrugs wurde. Roman wollte eigentlich Geld aus seinen Devisen an sich überweisen, gelangte jedoch auf eine täuschen echte Phishing-Seite im Paypal-Stil. Er verlor dadurch 100.000 Rubel (ca. 1.400 Euro), die ihm von den Betrügern während des Vorgangs gestohlen wurden. Roman erinnerte sich später daran, dass er für die Überweisung auf die Zwei-Faktor-Verifizierung via SMS verzichtet hatte, einen Unterschied zur Original-Website hatte er in dem Moment nicht feststellen können. Grade weil es so schnell geht, sollten Sie Ihre Daten mit allen erdenklichen Mitteln schützen.

Viele Phishing-Seiten sind kaum bis gar nicht von der Original-Website zu unterscheiden. Besonders beim Surfen mit dem Handy wird die Erkennung noch schwieriger. Wie also soll man die Original-Website erkennen, und wissen, dass man ihr vertrauen kann?

Den ersten Unterschied zu einer Phishing-Seite erkennen Sie in der URL, also der Adresse in der Zeile oben im Browser. Es wird dabei von den Hackern versucht, eine ähnliche Adresse zum Original zu finden. Teilweise sind die Websites nur für wenigen Tage aktiv. Statt https://paypal.com/ steht in der Adresszeile zum Beispiel:

·t.paypal.com

·paypal-visa.com

·paypai.co

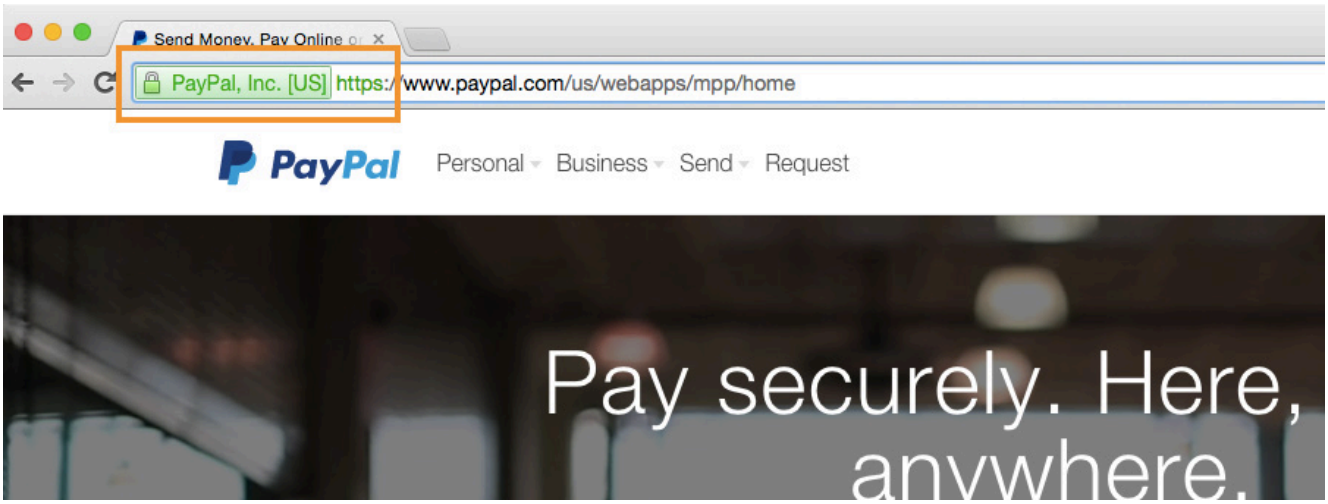
·paypal.hk

·paypl.co

Wie gelangen Internetnutzer auf diese Websites? Vor allem bei der Suche in Suchmaschinen werden die Top-Platzierungen mit Werbemitteln gekauft. Diese bezahlten Links müssen nicht zwingend etwas mit dem eigentlich gesuchten Service zu tun haben, und werden deshalb auch von Hackern genutzt. Weil der Name jedoch ähnlich ist, übersehen einige Nutzer die fehlerhafte URL.

Der zweite Unterschied zu einer Phishing-Seite ist das fehlende SSL-Zertifikat. Heutzutage arbeiten alle Websites, auf denen Sie vertrauliche Daten eingeben können, mit einem HTTPS Protokoll zur sicheren Datenübertragung. Die allermeisten Phishing Websites nutzen hingegen noch das unsichere http-Protokoll. Solchen Seiten können Sie im Hinblick auf eine sichere Datenübertragung grundsätzlich nicht vertrauen.

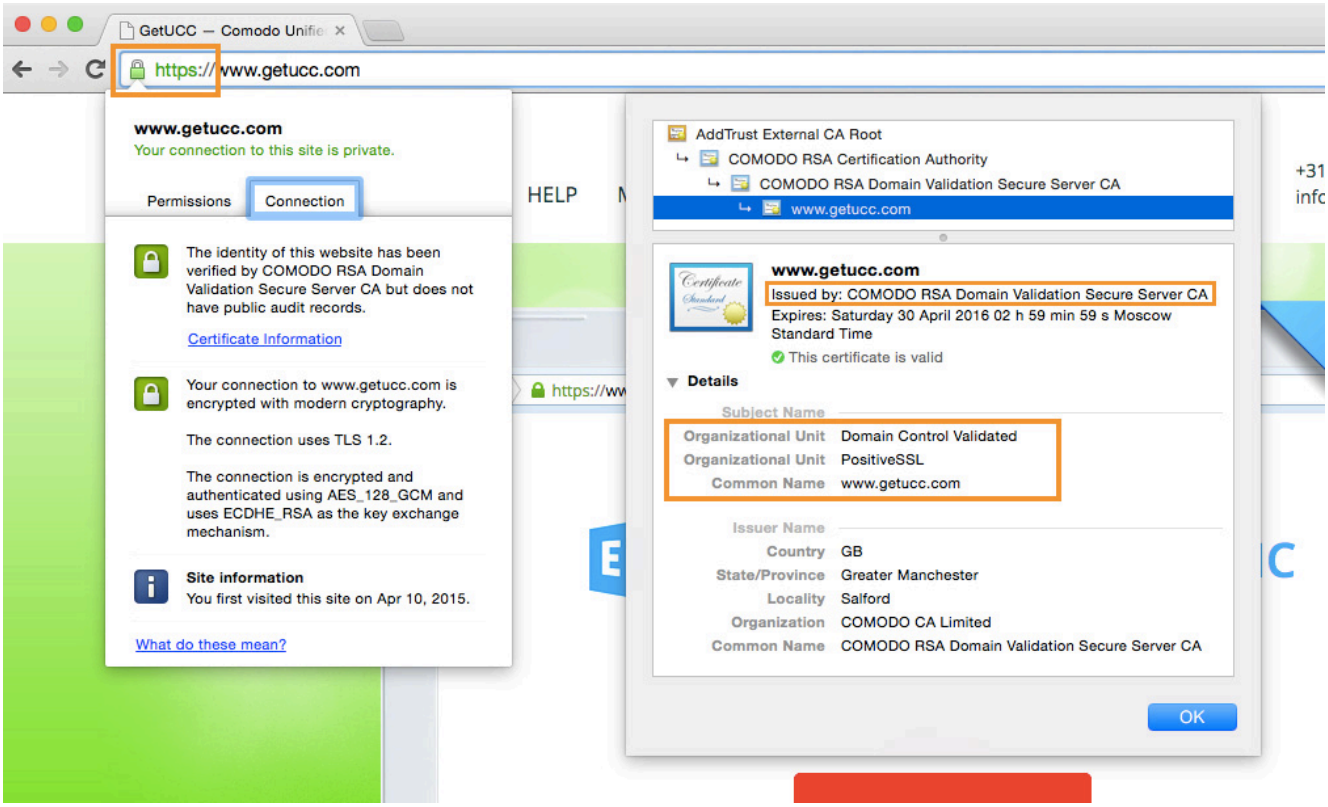
Auf einer sicheren Website sehen Sie ein Schloss-Symbol in der linken Ecke der Adresszeile des Browsers. Wenn Sie auf dieses Symbol klicken, erhalten Sie weitere Details über das Zertifikat.



Leider nutzen zurzeit auch erste Phishing-Seiten eine gesicherte Datenübertragung und das Schloss-Symbol. In diesem Fall gilt es, ein besonderes Augenmerk auf die Art des Zertifikats zu legen: ein DV-Zertifikat schütz zwar die Daten bei der Übertragung, trifft aber keine Aussage über die Echtheit des Unternehmens selbst (z.B. Paypal).

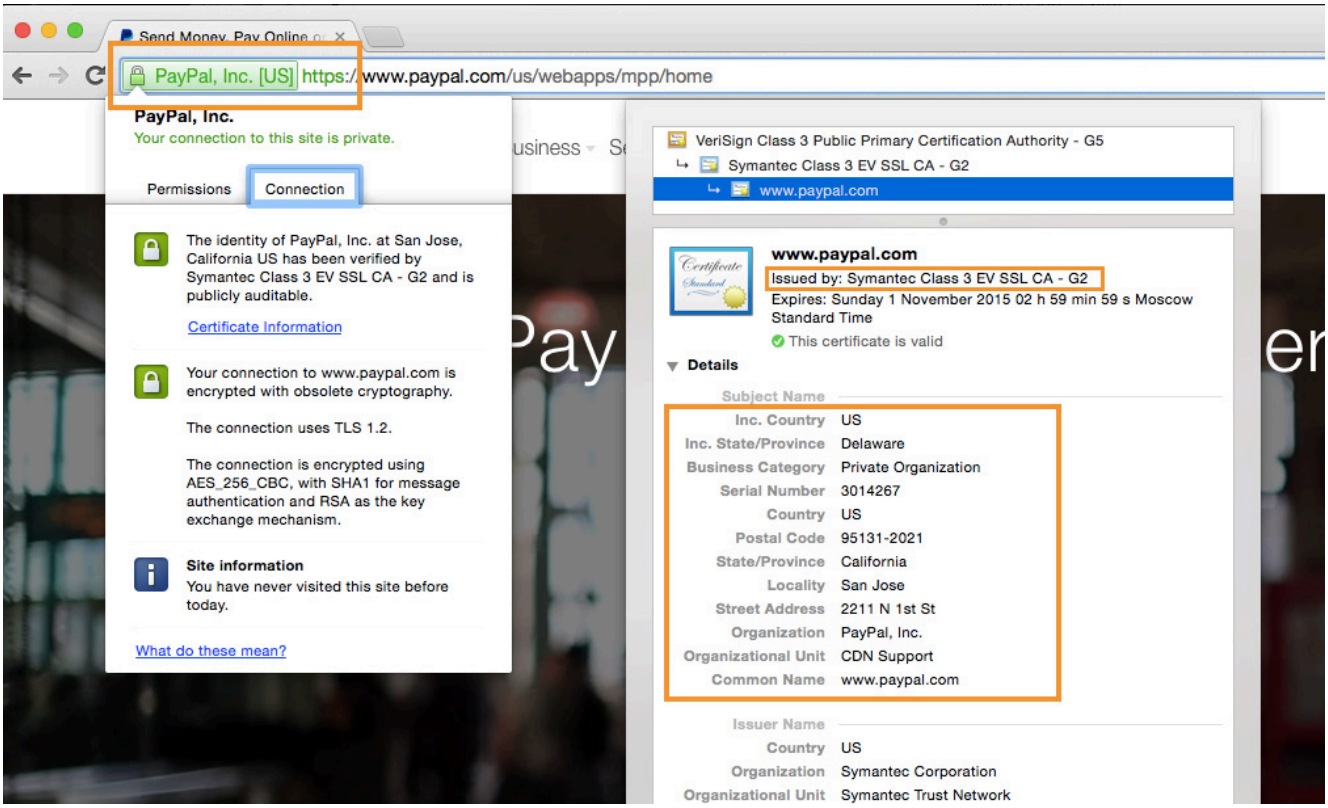
Ein EV-Zertifikat hingegen garantiert nicht nur den sicheren Datenaustausch, es zeigt neben dem Schloss-Symbol auch den Namen des Unternehmens, welches zuvor geprüft wurde. Damit sind EV-Zertifikate die aktuell sichersten und vertrauenswürdigsten Zertifikate.

Zudem färbt das Zertifikat einen Teil der Adresszeile grün und signalisiert damit jedem Nutzer die garantierte Sicherheit dieser Seite.



SSL-Zertifikat: Zum Schutz für Unternehmen

Jedes Unternehmen, welches im Internetdienste anbietet und dabei sensible Nutzerdaten verarbeitet, sollte zum größtmöglichen Schutz der Kunden ein EV SSL-Zertifikat einsetzen.



Durch den Einsatz dieses Zertifikats werden alle Informationen verschlüsselt übertragen, indem sie vor der Übermittlung in eine Buchstaben/Zahlen-Kombination umgewandelt werden. Ein Hacker könnte mit diesem Code nichts anfangen.

Unternehmen mit einem EV-Zertifikat berichten, dass sie ihren Verkauf im Bereich eCommerce zwischen 10-40% steigern konnten – das bestätigen auch unabhängige Analysten. Kaufen Sie Ihr EV-Zertifikat gleich hier.