Sophos klärt auf: Vorsicht iTunes User! Der fiese Trick mit dem falschen AppStore und woran man ihn erkennt

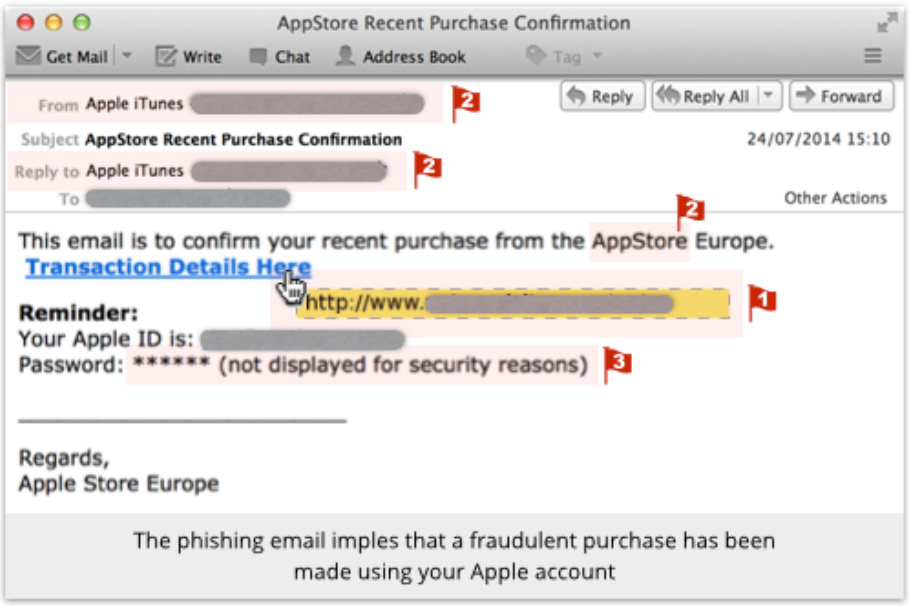
Phishing ist mittlerweile weithin bekannt. Und doch fallen immer wieder unzählige Menschen darauf rein. Denn manche Dinge, die einem ganz normal erscheinen, sind es bei näherer Betrachtung nicht. Ein falscher Apple „Appstore“ zum Beispiel, falsche Zahlvorgänge etc. Bei vielen Betrugsversuchen gibt es Warnhinweise, beispielsweise auf gefälschte E-Mails oder Webseiten, die leicht zu erkennen sind. Hier ein typischer Fall:

Eine typisches iTunes-Phishing

Der vorliegende Betrugsversuch startete mit einer Mail, die angeblich von Apple kam. Über den App Store und iTunes werden unzählige Käufe getätigt und so wird die Marke Apple bei Betrügern zusehends beliebter. Die Chance, dass ein Nutzer bereits einmal bei iTunes oder im Apple Store eingekauft hat, ist relativ hoch.

→ Im Jahr 2011 untersuchte Sophos fast 15.000 Typosquats (absichtlich falsch geschriebene Domainnamen) für sechs Marken. 86 Prozent der Fehler bei der Eingabe von apple.com hatten einen kriminellen Hintergrund.

Mit unserer vorliegenden E-Mail versuchten die Betrüger dem Verbraucher zu suggerieren, dass jemand Fremdes den Account gehackt und Einkäufe darüber getätigt hat. Das perfide: es stimmt nicht – noch nicht.



Die roten, mit Nummern versehenen Zahlen zeigen die Warnhinweise:

- Fehlerhafte Links: unwahrscheinliche Domainnamen, fehlendes HTTPS Protokoll oder sogar beides.
- Unwahrscheinliche oder fehlerhafte Inhalte: Rechtschreibfehler und Inkonsistenzen.
- Elemente, die dort nicht hingehören: falsche Informationen werden angefordert oder angezeigt.

Die Urheber hoffen nun, dass die User auf einen der Links klicken, der vermeintlich zur Klärung der Transaktion beiträgt.

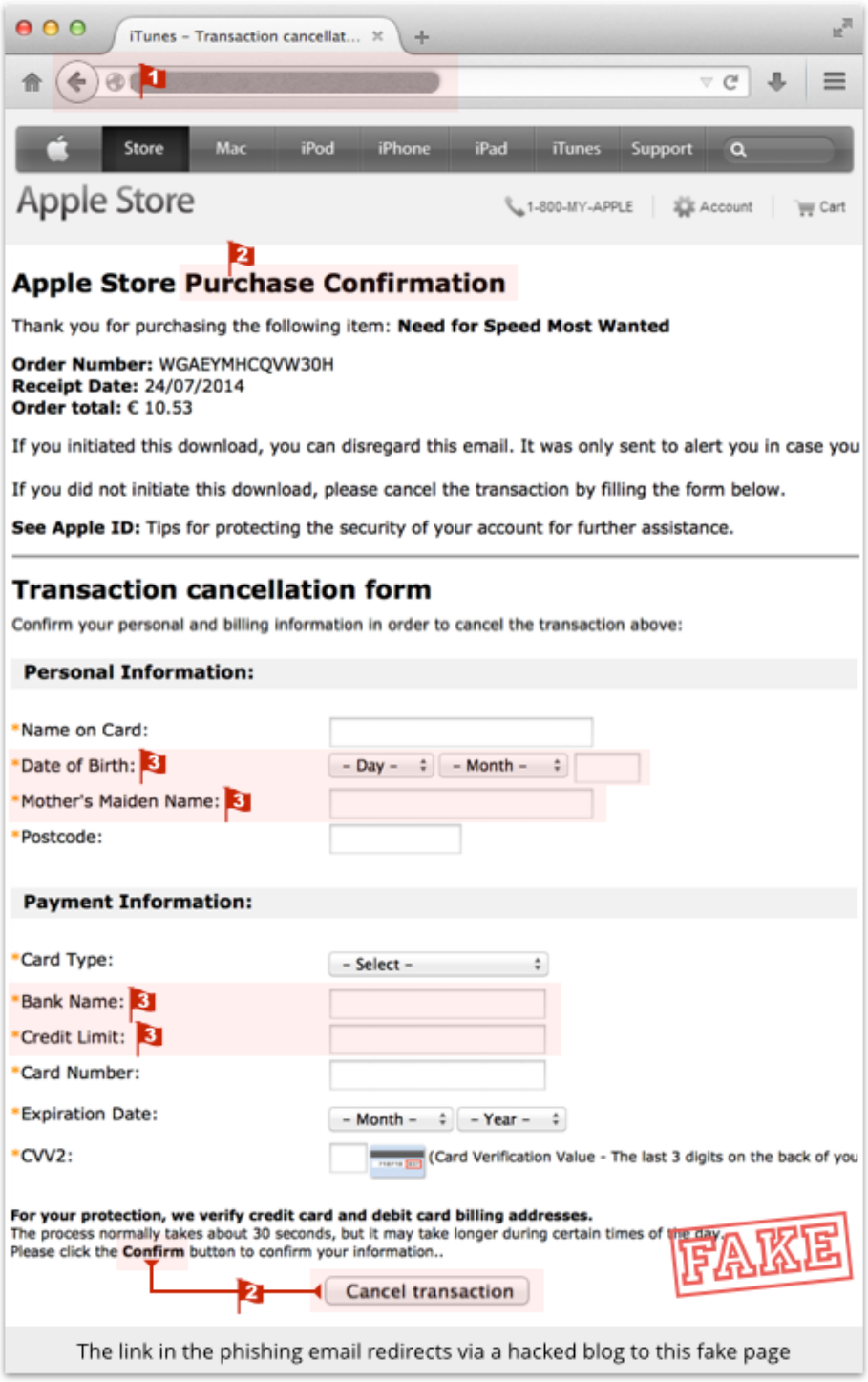
Die tatsächliche Aufgabe der roten Flaggen:

- Ein Blick auf den Link zeigt, dass dieser nicht von Apple ist. Er führt zu einer legitimen Webseite, die gehackt wurde.
- Die E-Mail-Adressen von Absender und „Antwort an“-Empfänger gehören ebenfalls nicht zu Apple und werden für offizielle E-Mails des Herstellers auch nicht verwendet.
- Es ist nicht der „AppStore“, es ist der „App Store“.
- Apple kann die Kennwörter seiner Kunden verifizieren, aber nicht wiederherstellen. Das Unternehmen speichert niemals Passwörter und würde auch nie behaupten, dass es dies tut und dem Nutzer ein vergessenes Passwort zusenden kann.

Der gefälschte Apple Store

Klickt der Verbraucher nun auf die Transaktionsdetails landet er auf einer Webseite, die Parfüms und Düfte verkauft.

Zwar handelt es sich bei dieser um ein legales Geschäft, allerdings basiert die Seite vermutlich auf einer unsicheren Version von WordPress. So können Kriminelle ihren Content einfügen und haben Gelegenheit, einen ansonsten seriösen Domain-Namen für ihre Zwecke zu nutzen.



Die gehackte WordPress-Website leitet dann im Hintergrund des Browsers auf die richtige Phishing-Seite und vermittelt mit ein paar grafischen Elementen von Apple den Eindruck es handle sich um die Originalseite.

Auch hier gibt es rote Flaggen in allen Kategorien:

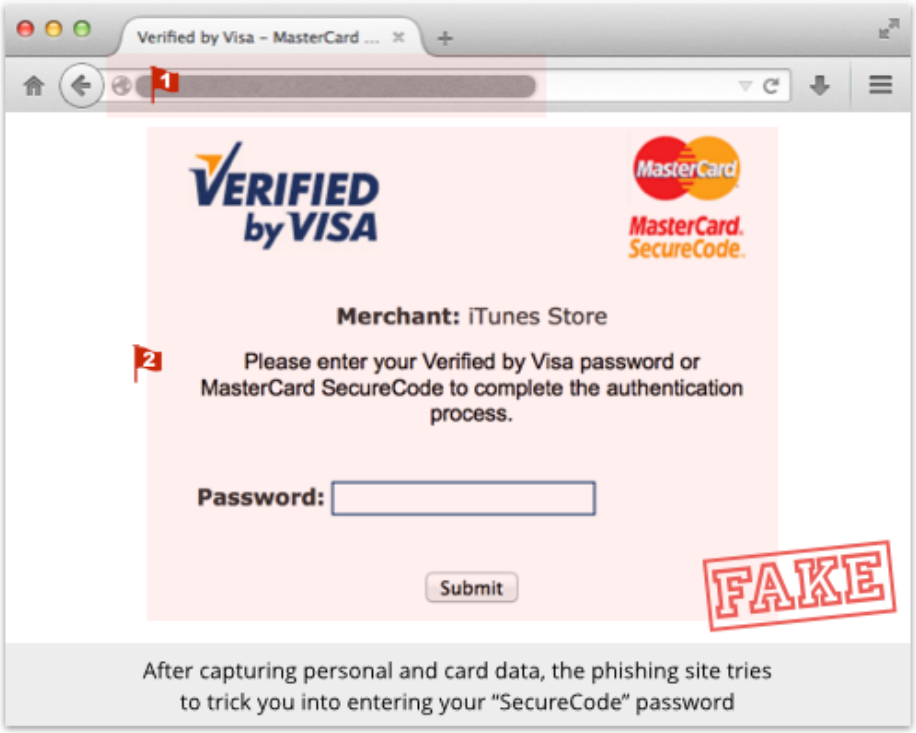
- Eine URL die nicht von Apple ist und die vertrauliche Informationen auf einer unsicheren (nicht HTTPS)-Seite anfordert.
- Inkonsistenzen in der visuellen Darstellung, wahrscheinlich aufgrund schlampig ausgeführtem Copy-und-Paste durch die Gauner. So beschreibt beispielsweise die Überschrift "Kaufbestätigung" nicht den Rest der Seite und die Funktion „Transaktion Abbrechen“ heißt "Kauf bestätigen".
- Auch Fragen, die normalerweise niemals im Zusammenhang mit einem Zahlungsvorgang gestellt werden, weisen auf kriminelle Machenschaften hin, so die Frage nach dem Kreditlimit oder dem Mädchenname der Mutter .

Fehler in einer Web-Seite sind in aller Regel ein Indikator für Phishing. Aber auch mit Seiten, die völlig ohne Fehler daherkommen, kann etwas faul sein.

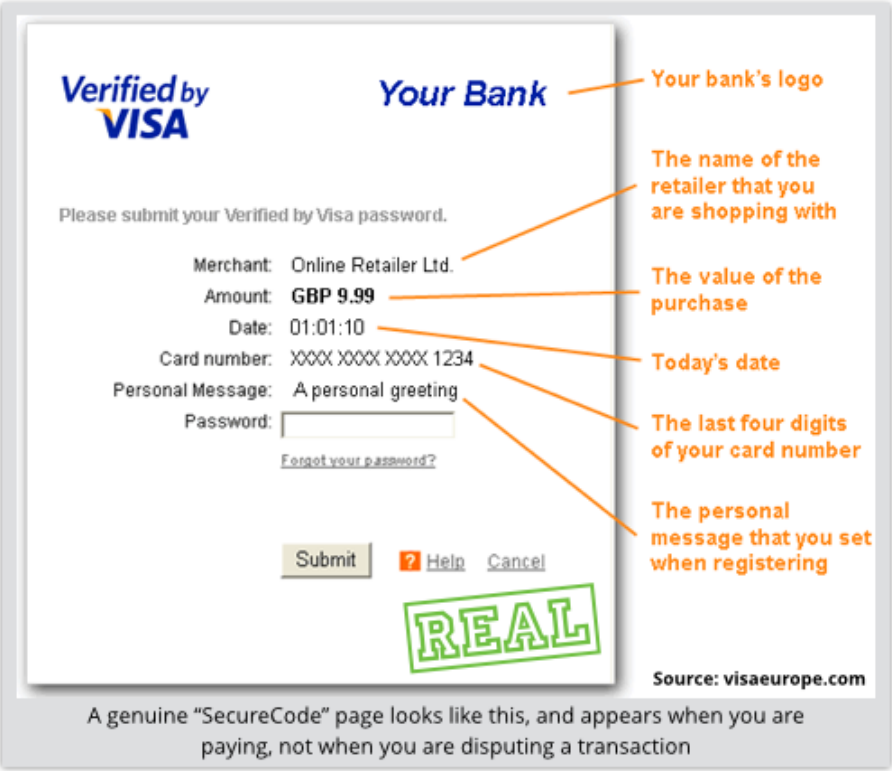
Die gefälschte "SecureCode" Bildschirm

Bisher haben die Gangster also schon eine Menge persönlicher Daten erhalten können. Als nächstes versuchen sie, diese über den VISA oder MasterCard SecureCode zu verifizieren.

SecureCode ist ein sekundäres Authentifizierungssystem, das den Käufer in einem extra Schritt als Karteninhaber identifiziert. Dieser Code wird nur direkt an VISA oder MasterCard, nicht an den Händler übermittelt.



Auf der hier gezeigten Beispielseite ist so gut wie alles verkehrt, denn der Security Code wird nie von Händlern (als Ausführer der Transaktion) sondern immer von den Finanzunternehmen selbst abgefragt. In diesem Fall dürften die Verbraucher gar keine Seite zur Validierung sehen weil dem Bezahlvorgang keine Transaktion vorangegangen ist.



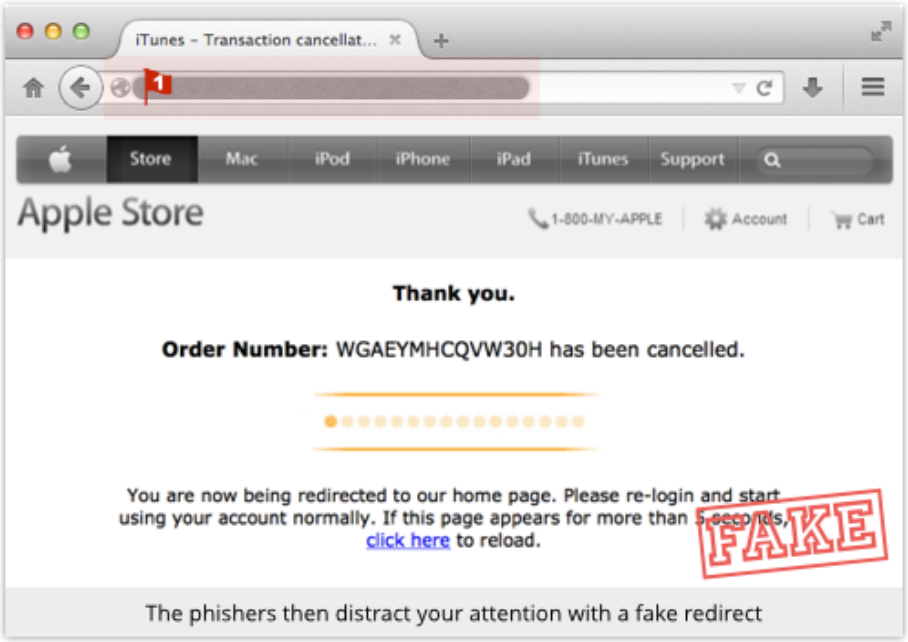
A genuine "SecureCode" page looks like this, and appears when you are paying, not when you are disputing a transaction

Die Beruhigungsseite

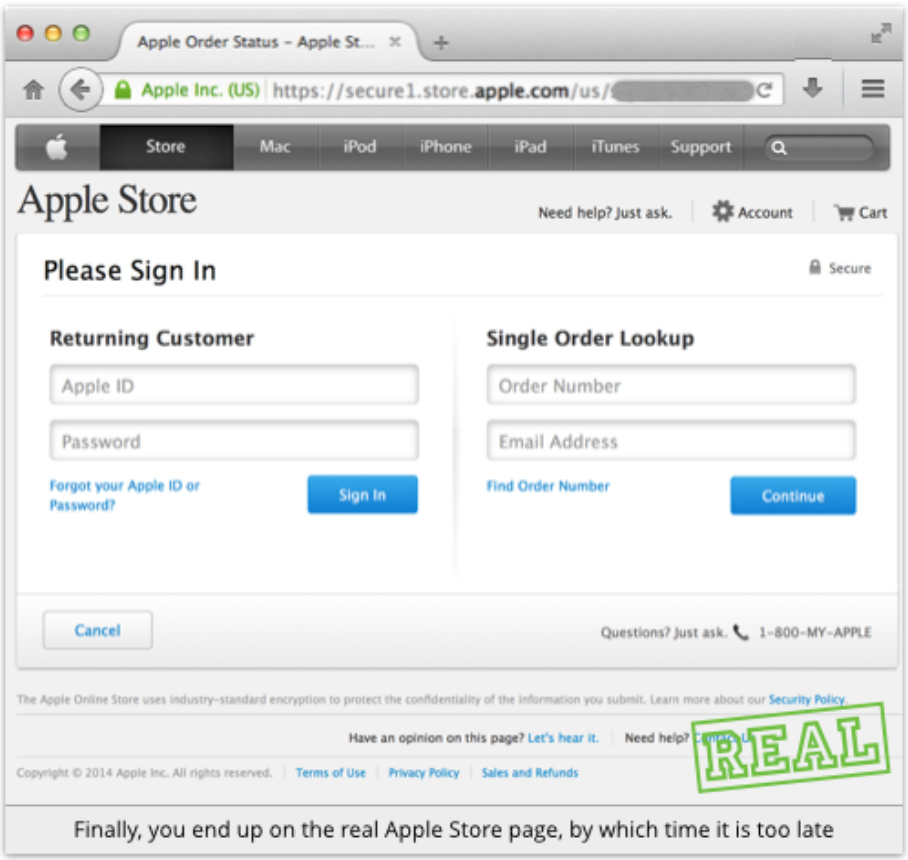
Mittlerweile haben die Betrüger die Kartendaten und das SecureCode Passwort sowie genügend Informationen, um die Bank in einem Telefonat von ihrer Identität zu überzeugen.

Gelingt ihnen das, können sie möglicherweise Kontoauszüge umleiten, die Telefonnummer ändern, die Verbraucher für Benachrichtigungen und zwei-Faktor-Authentifizierung verwenden und den Inhaber sogar von seinem eigenen Account aussperren. Alle diese Dinge haben den Zweck, den Betrügern möglichst viel Zeit zu verschaffen, um das Konto leerzuräumen.

Damit betreten wir die letzte Phase des Phishing die den Verbraucher versichern soll, dass alles wie gewünscht läuft.



Diese Seite ist wirklich nur ein bisschen visuelles Theater, aber dennoch würde man erwarten, dass sie eine Apple-basierte URL hat und HTTPS verwendet. Um ein allzu plötzliches Ende zu vermeiden, wird der Kunde zum echten Apple Store umgeleitet.



Ironischerweise findet er hier, was er vorher hätte vermissen müssen: eine echte Apple URL und HTTPS .

Selbst jetzt haben die Verbraucher noch eine Chance, die Gauner zu schlagen, vor allem dann, wenn ihre Daten zum Verkauf angeboten werden sollten und nicht bereits für kriminelle Zwecke genutzt wurden.

Ein Anruf beim Kreditkartenanbieter unter der Nummer auf der Rückseite ihrer Karte kann Schlimmeres verhindern.

Weitere Infos zu diesem Thema oder zu Security allgemein finden Sie unter www.nakedsecurity.sophos.com.

Über Sophos

Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Sophos' Complete-Security-Lösungen als den besten Schutz vor komplexen IT-Bedrohungen und Datenverlust. Sophos bietet dafür preisgekrönte Verschlüsselungs-, Endpoint-Security-, Web-, Email-, Mobile- und Network Security-Lösungen an, die einfach zu verwalten, zu installieren und einzusetzen sind. Das Angebot wird von einem weltweiten Netzwerk eigener Analysezentren, den SophosLabs, unterstützt.

Sophos hat seinen Hauptsitz in Boston, USA, und Oxford, Großbritannien. In Deutschland hat das Unternehmen seinen Hauptsitz in Wiesbaden und ist in Österreich und der Schweiz je an einem Standort vertreten. Weitere Informationen unter www.sophos.de.

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Christiane Capps, +49-174-3335550
Ulrike Masztalerz, +49-40-484434
sophos@tc-communications.de