Pishing:
Immer raffiniertere Betrugsversuche

https://www.beobachter.ch/digital/sicherheit/phishing-immer-raffiniertere-betrugsversuche

Immer wieder versuchen Internet-Betrüger, mit gefälschten Mails an Geldzahlungen oder sensible Daten zu kommen. Welche Phishing-Mails aktuell im Umlauf sind, sehen Sie hier.

Falsche SMS im Namen der Migros

Achtung: Zurzeit werden falsche SMS mit der Migros als Absender verschickt. Der Empfänger der Nachricht soll bei einer Postleitzahl-Ziehung zu den glücklichen Gewinnern gehören und dafür auf einen Link klicken. Die Migros warnt, dass die Nachricht gefälscht sei und man den Short-Link nicht aufrufen solle. Derartige Nachrichten seien immer mal wieder im Umlauf. Seit dieser Woche sind die Betrüger aber vermehrt aktiv, weshalb sich einige Besorgte bei Migipedia, dem Migros-Forum, sowie auf Twitter gemeldet haben (siehe unten). Auch dem Beobachter wurde ein Fall gemeldet.

Deshalb ist die beste Reaktion auf die SMS: sofort löschen!

Update vom 19.10.2018

Hey Sarah. Nein das tun wir tatsächlich nicht. Ist leider ein Fake und führt auf eine Seite, die deine Daten will. Hast du das heute erhalten? Unser Rechtsdienst ist bereits informiert. Merci für die Meldung. ^dv

— Migros (@migros) 16. Oktober 2018

Was ist Phishing?

Das Wort Phishing setzt sich aus den englischen Wörtern «Password», «Harvesting» und «Fishing» zusammen. Mittels Phishing versuchen Betrüger, an vertrauliche Daten von ahnungslosen Internet-Benutzern zu gelangen. Dabei kann es sich beispielsweise um Kontoinformationen von Online-Auktionsanbietern (zum Beispiel eBay) oder Zugangsdaten für das Internet-Banking handeln.

Die Betrüger nutzen die Gutgläubigkeit ihrer Opfer aus, indem sie ihnen E-Mails mit gefälschten Absenderadressen zustellen. In den E-Mails wird das Opfer beispielsweise darauf hingewiesen, dass seine Kontoinformationen und Zugangsdaten (zum Beispiel Benutzernamen und Passwort) nicht mehr sicher oder aktuell sind und es diese unter dem im E-Mail aufgeführten Link ändern soll. Der Link führt dann allerdings nicht auf die Originalseite des jeweiligen Dienstanbieters (etwa der Bank), sondern auf eine vom Betrüger identisch aufgesetzte Webseite.

Mit den erschlichenen Daten kann ein Betrüger im Namen des Opfers beispielsweise Banküberweisungen tätigen oder Angebote bei einer Online-Versteigerung platzieren.

Phishing-Attacken zielen auf die Herausgabe persönlicher Daten

Das klassische Phishing, bei dem Opfer in E-Mails dazu verleitet werden, sensible Daten wie Kreditkartendaten anzugeben, ist auf dem Vormarsch. In den letzten Jahren kamen aber auch zahlreiche Voice-Phishing-Angriffe hinzu, die gegen Schweizer E-Banking-Kunden gerichtet waren (siehe Bild unten): Dabei werden Phishing-E-Mails versendet, welche vorgeben, dass das Finanzinstitut zum Schutz des E-Banking-Kontos ein neues Sicherheitssystem installiert hat. Ein Bankmitarbeiter werde sich mit dem Opfer telefonisch in Verbindung setzen, um den Prozess zu diskutieren und zu vervollständigen. Zu diesem Zweck wird das Opfer gebeten, neben persönlichen Daten auch seine Telefonnummer anzugeben.

Anschliessend werden die Opfer von den Betrügern angerufen und unter dem Vorwand, die Sicherheit zu verbessern, dazu bewegt, das Passwort und das zweite Sicherheitselement anzugeben.

Dabei wird das Opfer beispielsweise aufgefordert, einen Code in den Kartenleser einzugeben und dem Angreifer das Ergebnis mitzuteilen. Mit diesen Angaben kann sich der Betrüger in das E-Banking-Konto

einloggen und eine Zahlung auslösen. Wird für das Auslösen der Zahlung die sogenannte Transaktionssignierung verlangt, wird der Prozess wiederholt und auch diese in der gleichen Art und Weise vom Betrüger erfragt. Der Telefonanruf wird jeweils professionell durchgeführt und erfolgt oftmals auch in Schweizerdeutsch. *(MELANI)*

Von: "RAIFFEISEN BANK AG"<info@Raiffeisen.ch>
Datum: 7. Mai 2013 09:22:43 MESZ
Betreff: Raiffeisen Kundendienst.

Sehr geehrter Kunde,

Kьrzlich, laut unseren Unterlagen, dass in Ihrer Raiffeisen Bank Account ein unbefugter Dritter hat versucht, in Ihr Konto einloggen. Die Sicherheit Ihres Kontos ist unser Hauptanliegen, so haben wir beschlossen, Beschrдnken Sie den Zugriff auf Ihr Konto vorьbergehend. Fьr den vollen Zugriff auf Ihr Konto, mьssen Sie Ihre Daten wiederherstellen, um das zu bestдtigen Link:
WWW.RAIFFEISEN.COM

Sobald Ihre Daten von uns ьberprьft wurden und bestдtigt, einer unserer personal wird Sie innerhalb von 48 Stunden per Telefon vollstдndig aktivieren Sie Ihr Konto und alle Zugang zu Ihrem Konto wird vollstдndig wiederhergestellt werden.

Vielen Dank fьr Ihre Mitarbeit.

Mit freundlichen GrьЯen,
RAIFFEISEN Bank AG Angelegenheiten Security Department.

Leicht erkennbarer Betrugsversuch: Seltsame Zeichen, seltsames Deutsch - ab in den Papierkorb.

Quelle: Thinkstock Kollektion

So schützen Sie Ihre Daten

- Geben Sie keine persönlichen Daten an, wenn Sie per E-Mail dazu aufgefordert werden, sondern löschen Sie die E-Mail.
- Beenden Sie umgehend Telefongespräche bei denen Sie nach Passwörtern, Kreditkartendaten oder anderen persönlichen Informationen gefragt werden. Keine Bank fordert ihre Kunden per Telefon oder E-Mail auf, Passwörter, Kreditkartendaten oder andere persönlichen Angaben anzugeben, zu verifizieren oder zu aktualisieren.
- Misstrauen Sie E-Mails, die Sie unaufgefordert bekommen.
- Besonders gerne werden E-Mail-Adressen vertrauenswürdiger Firmen für betrügerische Zwecke missbraucht.
- Kunden, welche Passwörter oder Kreditkartendaten wie oben beschrieben einem Betrüger angegeben haben, sollten sich umgehend an die E-Banking-Hotline der jeweiligen Bank wenden.

Wie Phishing-Mails melden?

- Wer als Privatperson Opfer einer Phishing-Attacke geworden ist und einen Schaden erlitten hat, sollte sich in erster Linie bei der lokalen Polizeistelle melden.
- Sind Firmen oder andere grosse Organisationen betroffen, können sich diese an die Melde- und Analysestelle Informationssicherung (Melani) wenden. Die Aufgabe von Melani ist es nicht, strafrechtliche Ermittlungen aufzunehmen. Dies ist Sache des Bundesamts für Polizei (Fedpol), das im Auftrag der Bundesanwaltschaft handelt. Anzeigen sollten Unternehmen bei der Kantonspolizei erstatten.
- Die Polizeistellen im Inland stehen in Kontakt mit dem Fedpol. Gehen die Ermittlungen über die Landesgrenzen hinweg, tauscht sich das Fedpol mit der zuständigen Polizei im Ausland aus.

Ist Phishing strafbar?

- Der blosse Versand von Phishing-Mails ist nicht strafbar.

- Erst wenn gegen ein bestimmtes Gesetz verstossen wird, erhält die verschickte Nachricht strafrechtliche Relevanz.
- Zu den Vergehen im Zusammenhang mit Phishing-Mails zählen folgende typische Straftatbestände: Urkundenfälschung (Art. 251 StGB), Geldwäscherei (Art. 305bis StGB) oder betrügerischer Missbrauch einer Datenverarbeitungsanlage (Art. 147 StGB). Mit letzterem ist gemeint, dass ein Angreifer beispielsweise in eine Datenbank eingreift, um dem Opfer mit den erhaltenen Daten einen Schaden hinzuzufügen oder um Geld zu entwenden.
- Das Fedpol ermittelt laufend bei Verfahren, die in Bundeszuständigkeit fallen. Dazu zählen zum Beispiel Wirtschaftsdelikte mit internationalem Bezug, terroristisch motivierte Verbrechen oder solche, die den Staat schädigen. Da Cyberdelikte über Kantons- und Landesgrenzen hinweg stattfinden, wurde ein nationales Cyberboard geschaffen. Das Cyberboard ist eine operative Plattform, die einen besseren Austausch und Koordination zwischen Bund (Bundesanwaltschaft, Fedpol, Melani) und den Kantonen (Kantonspolizeien, Kantonale Staatsanwaltschaften) ermöglicht.

Beispiele von typischen Phishing-Mails

Gefälschtes Login beim E-Banking

Melani warnt vor einer Betrugsmasche beim E-Banking.

Es geht darum, dass Kriminelle den Login-Vorgang beim E-Banking manipulieren. Mittels Social Engineering* werden Smartphone-Nutzer im Glauben gelassen, dass sie aufgrund eines Updates des Online-Banking-Systems die Informationen aus dem Aktivierungsbrief einsenden sollen. Diesen Brief schickt die Bank in der Regel bei der Anmeldung zum E-Banking an den Kunden, damit ein Zweitgerät für die mobile Authentifizierungsmethode zugelassen wird. Damit beabsichtigen die Phishing-Betrüger, an das farbige Mosaikbild zu kommen, welches das Opfer bereits für die Registrierung mit dem Smartphone gescannt hatte (siehe Bild unten).

Melani warnt, dass es den Betrügern dadurch unter Umständen möglich ist, sich in das E-Banking des Opfers einzuloggen, indem ein weiteres Smartphone für die sogenannte Zwei-Faktor-Authentifizierung aktiviert wird. Ab diesem Zeitpunkt können sich die Angreifer jederzeit in das E-Banking Portal einloggen und ohne das Wissen des Opfers Zahlungen auf ein Konto auslösen.

Diese Sicherheitsvorkehrungen sollten Sie beachten

Das sind die wichtigsten Tipps von Melani im Umgang mit E-Banking:

- Geben Sie Informationen aus dem Aktivierungsbrief nie weiter, auch nicht an die Bank. Dieser ist persönlich für den Kunden bestimmt. Im Zweifelsfall kontaktieren Sie die Bank direkt und fragen telefonisch nach.
- Stellen Sie sicher, dass Sie beim Login-Vorgang ins E-Banking auf dem mobilen Gerät (beispielsweise Smartphone oder PhotoTAN-Gerät) wirklich das Login bestätigen und dass es sich nicht bereits um die Visierung einer Zahlung handelt.
- Lesen Sie immer den ganzen Text auf dem mobilen Gerät, wenn Sie eine Zahlung visieren. Überprüfen Sie zur Sicherheit auch nochmals den Betrag und Empfänger (Name, IBAN) vor der Freigabe der Zahlung.

Wer Bedenken hat, bereits in die Falle der Angreifer getappt zu sein, sollte umgehend den E-Banking-Vertrag sperren lassen. Weitere Infos zur Sicherheit beim E-Banking finden Sie auf www.ebas.ch.

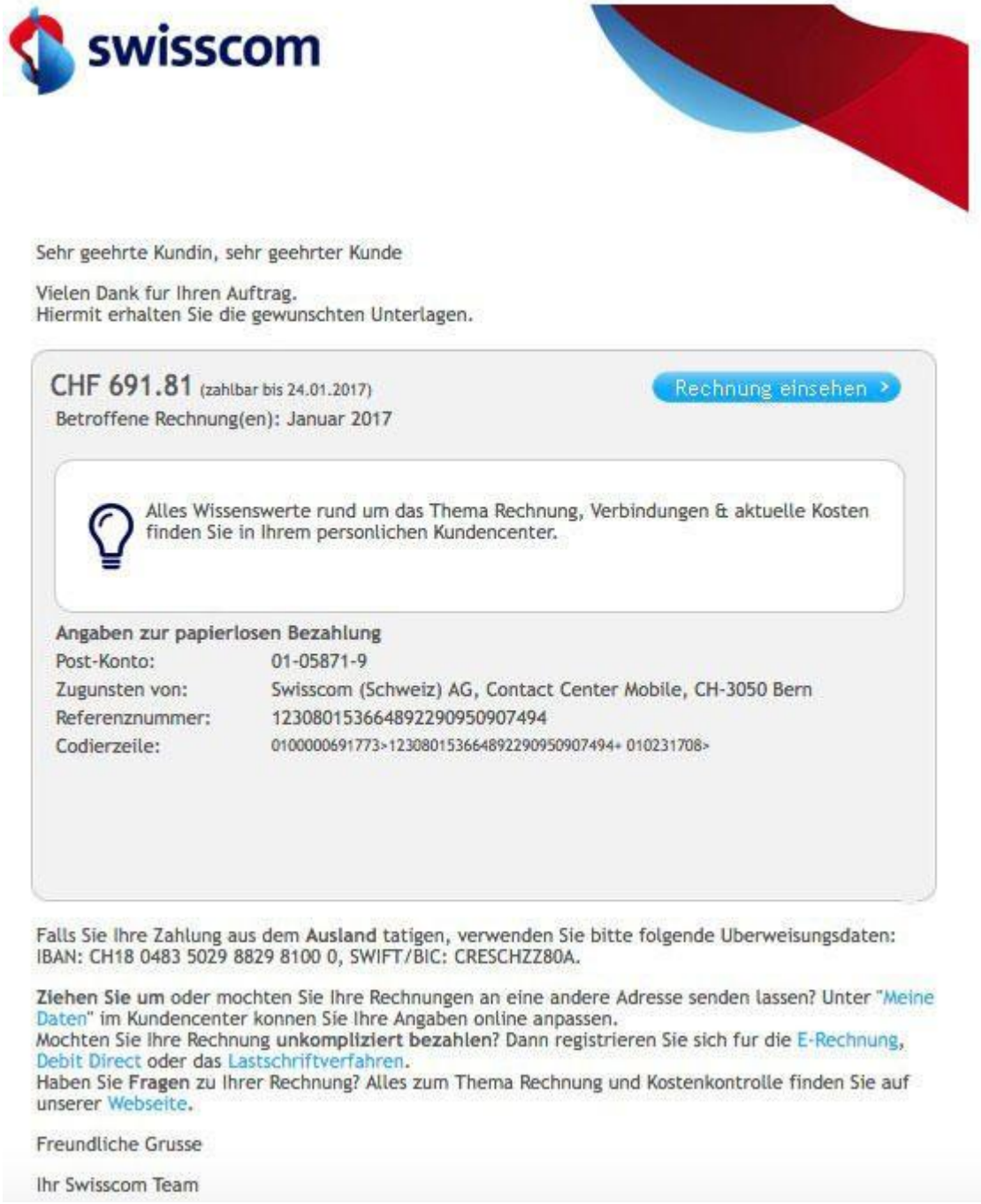
Klicken Sie für eine vergrösserte Darstellung auf das Bild. (Quelle: Melani)

*Social Engineering ist eine Hacking-Methode, welche die Gutgläubigkeit oder Unsicherheit von Personen ausnutzt. Dabei wird der Kunde beispielsweise aufgefordert, vertrauliche Daten preiszugeben, um angeblich eine Sicherheitslücke zu schliessen.

Gefälschte Rechnungskopie der Swisscom

Seit Anfang 2017 kursiert eine Phishing-Mail im Namen der Swisscom mit dem Betreff «Rechnungskopie». Dem Empfänger wird vorgegaukelt, dass er bei der Swisscom eine höhere dreistellige Rechnungssumme begleichen müsse. Bei einem Klick auf den Button «Rechnung einsehen» (siehe Bildausschnitt), läuft der Nutzer jedoch Gefahr, sich gefährliche Schadsoftware auf den Rechner zu laden.

Die Swisscom warnt explizit vor der Phishing-Mail und klärt auf, worin sich das Phishing-Mail von der unternehmensüblichen Kunden-Kommunikation unterscheidet.



Merkmale der Phishing-Mail:

1. Der Kunde wird nicht persönlich angesprochen, sondern nur mit «Sehr geehrte Kundin, sehr geehrter Kunde»
2. Rechnungsbeträge werden auf den Rappen genau ausgestellt (z. B. 691.81 oder 929.33 Franken). Die Swisscom rundet diese immer auf.
3. Umlaute wie ä, ö oder ü fehlen. Generell sollte man bei Mails mit Rechtschreibfehlern skeptisch sein, da standardisierte Benachrichtigungen an die Kunden mehrmals geprüft worden sind.
4. Scheint die Absender-Adresse für das Unternehmen wenig plausibel oder ist diese sehr lang, handelt es sich meistens um Phishing. Am Absender «sme.contactcenter@bill.swisscom.com» kann man relativ einfach erkennen, dass die Firma nicht über eine solche Mail-Adresse verfügt.

Inkasso im Auftrag von Amazon

Zu Weihnachten 2016 machte eine Zahlungsaufforderung über eine angeblich misslungene Buchung via Amazon die Runde. Der Empfänger der betrügerischen Mail-Nachricht sollte im Glauben gelassen

werden, dass die Überweisung für die Online-Bestellung nicht zustande gekommen sei (siehe Screenshot unten).

Ein Beobachter-Leser erhielt ein solches Schreiben per Mail. Im Anhang befand sich eine ZIP-Datei, die beim Öffnen mit grosser Wahrscheinlichkeit Schadsoftware auf den Rechner lädt.

So reagieren Sie richtig:

1. Öffnen Sie auf keinen Fall den Anhang, auch wenn Sie sich über den vermeintlichen Inhalt wundern. Entfernen Sie die E-Mail komplett aus Ihrem Posteingang.
2. Falls Sie in letzter Zeit etwas über Amazon bestellt haben, können Sie die Bestellnummer auch in Ihrem Kundenkonto nachprüfen.
3. Sind Sie unsicher, ob es sich um eine echte Nachricht von Amazon handelt, können Sie diese in der Regel auch im Message Center im persönlichen Kundenbereich finden. Melden Sie gefälschte Mail-Adressen direkt an den Versandhändler unter stop-spoofing@amazon.com.

Gefälschte Zahlungsaufforderungen

Im Sommer 2016 erhielten einige Konsumenten gefälschte Zahlungsaufforderungen per Mail. Manchmal sehen die Schreiben täuschend echt aus, manchmal aber sind sie derart schlecht formuliert, dass man sofort merken kann, dass etwas faul ist.

Nachfolgend zwei Beispiele solcher Schreiben, die uns von aufmerksamen Beobachter-Lesern zugesendet wurden:

Beispiel 1: «Aufmerkamkeit»

-----Original Message-----
From: "Denis Werneille" <ttiessen@t-online.de>
To: [redacted]
Date: Thu, 7 Jul 2016 13:46:30 -0700
Subject: [redacted] - Ihre Warenrechnung ist überfällig (# 19149588)

Lieber [redacted]
Ich hoffe, dass sie diese email erhalten. Ich möchte Sie daran erinnern, dass wir Ihnen eine Rechnung am 24.06 2016 gemailt haben. Wir haben bis dato keine Überweisung bekommen, deshalb schreibe ich, dass die email nicht versehentlich gelöscht wurde. Würden Sie so nett sein nachfragen ob die Finanzabteilung die Rechnung bekommen hat? Ich habe Ihnen ein Kopie der Rechnung beigefügt. Wir würden uns sehr freuen, wenn Sie Rechnung in der nächsten Woche überweisen könnten.
Ich danke Ihnen sehr für Ihre Aufmerkamkeit! Mit freundlichen Grüssen.
Denis Werneille
FinanzdatenanalystIn.
Novartis Pharma AG
+412279225[redacted]
Industriestrasse 34, 9463, St. Gallen, Switzerland

Hier fällt auf:

1. Zahlreiche Schreibfehler und fehlerhaftes Deutsch.
2. Adresse gibt es nicht. Die Industriestrasse in St. Gallen endet bei der Nummer 14.
3. Postleitzahl 9463 ist falsch. Diese gehört der Gemeinde Oberriet SG.
4. Telefonnummer ist falsch. Bei einem Anruf unter +412279225** landet man bei einem Privathaushalt in Prévenloup/VD.

Beispiel 2: «Höflich darauf hinweisen»

Von: Christian Juillerat [mailto:infos2020@t-online.de]
Gesendet: Donnerstag, 7. Juli 2016 23:00
An: [redacted]
Betreff: [redacted] Ihre Faktur ist überfällig (# [001771933]

Sehr geehrter [redacted]

Gerne möchten wir Sie höflich darauf hinweisen, **die am 25.Juni 2016** ausgestellten Rechnung von Werthenstein BioPharma GmbH über den Betrag am 14.Juli 2016 spätestens beglichen werden sollte.

Auftragsnummer: **#CH-01890067**
Gesamtbetrag: **€1,574.00**

Zu Ihrer Information haben wir dieser E-Mail eine Kopie der Rechnung beigelegt.

Ich wäre Ihnen dankbar, wenn Sie die ausstehende Rechnung bis zum 14.Juli 2016 begleichen könnten. Wir weisen Sie höflich darauf hin, dass bei zu später Begleichung des offenen Betrags Ihr Konto vorübergehend deaktiviert werden kann und bitten Sie daher, , uns schnellstmöglich zu kontaktieren um eine Unterbrechung der Dienstleistungen zu vermeiden.

Bitte zögern Sie nicht mich zu kontaktieren, falls Unklarheiten oder weitere Fragen bestehen.

Freundliche Grüsse,

Christian Juillerat,
Hauptbuchhalter
Werthenstein BioPharma GmbH

Hier fällt auf:

1. Im Text hat es einige Schreibfehler. Und die Art, wie der Brief formuliert ist, ist für geschäftliche Korrespondenz ungewöhnlich.
2. Auch die Anrede im Betreff ist ungewöhnlich. «Vorname.Name – Ihre Faktur ist überfällig» schreibt keine seriöse Firma in die Betreffzeile.
3. Die Adresse des Absenders «infos2020@t-online.de» ist verdächtig. Warum würde eine seriöse Firma einen t-online-Account benutzen?
4. Die Firma Werthenstein BioPharma GmbH gibt es tatsächlich, sie hat Sitz in Schachen LU und ist Teil des Chemiekonzerns Merck Sharpe & Dome MSD. Allerdings fehlen hier Kontaktadresse und Telefonnummer, was zwingend in ein offizielles Mail gehören würde.
5. Anhang keinesfalls öffnen! Es könnte sich um ein infiziertes Dokument handeln.

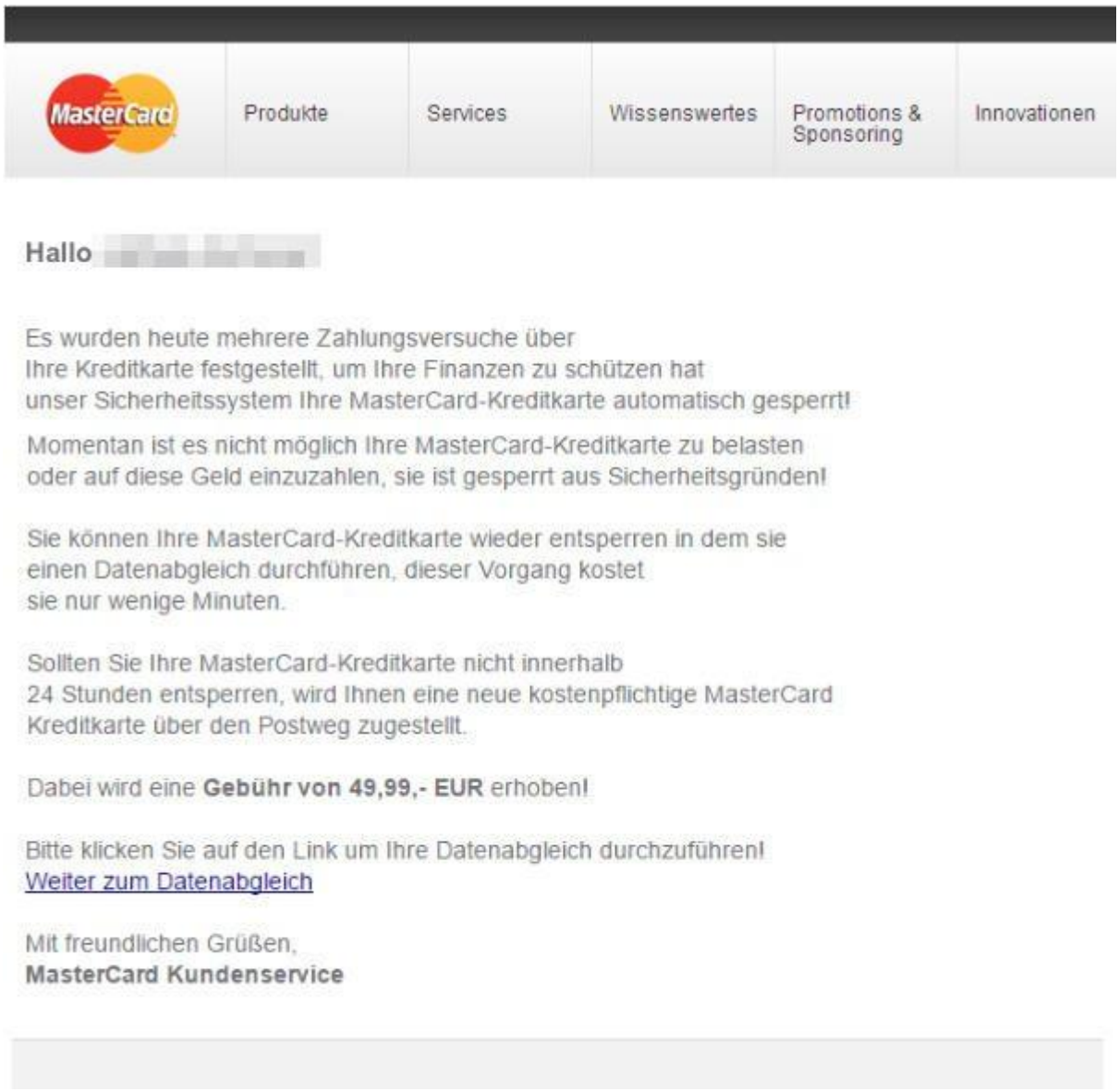
Professioneller Betrug mit Mastercard-Mail

Eine Leserin leitete uns eine Phishing-Mail weiter, welches im Namen von Mastercard versandt wird. Darin wird der Empfänger auf ungewöhnliche Zahlungsaktivitäten mit seiner Mastercard aufmerksam gemacht. Um die Finanzen des Kunden zu schützen, sei die Karte nun gesperrt worden, heisst es.

Dann folgt der Betrugsversuch: Um die Mastercard zu entsperren, sei ein Datenabgleich nötig. Dazu müsse der Kunde auf den aufgeführten Link klicken und dann seine Daten eingeben. Ein Vorgang, der nur wenige Minuten dauere.

Um die Kunden zum Klick zu bewegen, werden ausserdem Zusatzkosten in Aussicht gestellt. «Sollten Sie Ihre Mastercard-Kreditkarte nicht innerhalb (von) 24 Stunden entsperren, wird Ihnen eine neue, kostenpflichtige Mastercard-Kreditkarte auf dem Postweg zugestellt», schreiben die Betrüger.

Das vorliegende Phishing-Mail fällt besonders durch die professionelle Schreibweise und Gestaltung auf. Abgesehen von ein paar Fehlern im Satzaufbau, ist der Inhalt des Mails kaum von einer professionellen Mitteilung zu unterscheiden. Auch die Aufmachung des Designs lässt kaum Rückschlüsse auf einen Betrugsversuch zu. Trotzdem ist das Mail ein Betrugsversuch. Deshalb gilt: Finger weg, nicht öffnen und direkt in den Papierkorb verschieben.



Ein Betrugsversuch via Mastercard.

Quelle: Thinkstock Kollektion

Datenklau mit gefälschten Zalando-Mails

Markus Traber* aus Zürich staunte, als er vom Onlineshop Zalando eine E-Mail mit dem Betreff «Ihre Bestellung» erhielt: Er hatte noch nie etwas bei Zalando bestellt. Eine Nachfrage ergab schnell, dass Zalando nicht der Absender war – «sehr wahrscheinlich handelt es sich um eine Phishing-E-Mail», so Sprecher Matthias Ernst. Über eine angehängte Datei sollen Empfänger dazu gebracht werden, vertrauliche Daten einzugeben, etwa zu ihrer Kreditkarte. «Zalando bittet Kunden nie per E-Mail um vertrauliche Kundendaten oder Passwörter», so Ernst. Experten raten, E-Mails immer kritisch anzusehen und beim geringsten Zweifel an der Echtheit weder Anhänge zu öffnen noch sich auf Websites weiterleiten zu lassen.

Liste mit Phishing-Mails, die aktuell im Umlauf sind

In dieser Liste finden Sie Phishing-Mails, die aktuell im Umlauf sind und uns von Beobachter-Lesern gemeldet wurden. Die Liste erhebt keinen Anspruch auf Vollständigkeit: Wenn eine E-Mail nicht in der Liste aufgeführt ist, heisst das nicht, dass sie «sauber» ist.

Absender	Betreff	E-Mail
Amazon.de (updatekonto@amazon.de)	Ihr Konto Amazon.de	ansehen
Amazon.de (Account@amazon.de)	Wir haben vor kurzem festgestellt, dass verschiedene Computer zu Ihrem Amazon-Konto	ansehen
BKB E-BANKING (enquires@bkb.ch)	Wichtige	ansehen
BNP PARIBAS FORTIS (d.fedoce@meyer.it) (eduardolima@ifce.edu.br)	Dringend aandacht nodig!	ansehen
Corner (infos@corner.ch)	Mitteilung	ansehen
Credit-Suisse (info@credit-suisse.ch)	#90623 Konto Upgrade	ansehen
CREDIT SUISSE (notification.alert.online@credit-suisse.ch)	Sicherheit und Datenschutz	ansehen
CREDIT SUISSE GROUP AG (credit.sussie.mtan@credit-suisse.com)	Wichtige Mitteilung - mTAN deaktiviert	ansehen
CREDIT SUISSE GROUP AG (aktualisieren@credit-suisse.com)	m-Tan Sicherheit und Datenschutz!	ansehen
Eidgenössische Steuerverwaltung (berechnun@spport.com)	HINWEIS DER STEUERERKLÄRUNG FÜR DAS JAHR 2016	ansehen
FedEx Delivery Company Italy (jochoa@muniate.gob.pe)	Delivery Notification	ansehen
Fundsxpress (secure.fundsxpress.com)	Merchant Statement	ansehen
GeMoney Bank (secure@ge.com)	Wir brauchen, um Ihre Kreditkarten-Daten zu bestatigen!	ansehen
Groupe UBS AG (ch@ubs.ch)	3D-Secure-Aktivierung	ansehen
Linkedin (yom_alob3a@yahoo.com)	important message	ansehen
Microsoft (Secure Admin <message@windows.com>)	Secure your email	ansehen
PayPal (Kontakt@paypal-steuerns.ch)	Dringend : Ihr Antragsformular fur die	ansehen

Absender	Betreff	E-Mail
	Erstattung Paypal : (PP-FS-684-08-T2)	
PayPal (service@paypal.de <service@paypalsecure.de>)	Wichtig: Ungewöhnliche Aktivitäten in Ihrem PayPal-Konto (Ref #PP-571-010-574-467)	ansehen
PayPal (Director@Paypal-Client.de)	Dringend : Jahresgebühr für eine unbezahlte Rechnung Paypal.Fr !	ansehen
PayPal (Service@paypal.fr)	Votre Carte Bancaire est suspendue !	ansehen
PayPal (service@paypal.ch)	Der Zugriff auf Ihr Konto wurde eingeschr?nkt.	ansehen
PayPal Services (services@intl.paypal.com)	Reminder: Your account will be suspended until we hear from you?	ansehen
Pinnacle (Rechnungsstelle <info@pinnacle.com>)	Ihre Rechnung 1641157487 vom 13.05.2013	ansehen
Raiffeisen Bank (noreply.ch@raiffeisen.com)	Konto Aktualisieren	ansehen
RAIFFEISEN BANK AG (info@Raiffeisen.ch)	Raiffeisen Kundendienst	ansehen
Raiffeisen Schweiz (e-banking@raiffeisen.ch)	Konto Re-Aktivierung nötig	ansehen
Raiffeisen AG (info@raiffeisen.ch)	Raiffeisen Alert - Your Internet Banking gesperrt	ansehen
Raiffeisen Schweiz (raiffeisen@docksidela.com)	#990634 Raiffeisen E-Banking-Vertrag gesperrt.	ansehen
Reiffeisen E-Banking (mailservices@raiffeisen.ch)	Betreff: Ihre E-Banking wird in Kürze auslaufen.	ansehen
SONY Europe Limited / LCC & Solicitors (clerks@lccsolicitors.com)	Sonycoupon (prize of £1million)	ansehen
Sparkasse Bank (Kawano, Ruth (IHS/NAV) <rkawano@fdihb.org>)	Sparkasse Bank Wichtige Mitteilung	ansehen
Sparkasse Bank Germany (batorovak@nic.fns.uniba.sk)	Sparkasse Bank Benachrichtigung - Ihre Internet-Banking gesperrt	ansehen
Sparkasse (cucchim@d62.org)	Sparkasse Kundendienst	ansehen

Absender	Betreff	E-Mail
Swisscom (sme.contactcenter@bill.swisscom.com)	Rechnungskopie	ansehen
Timeshop24.de Ltd (Assistenz@timeshop24.de)	Eingang Ihrer Zahlung an Timeshop24.de Ltd.	ansehen
"UBS AG" <info@ubs.com>	UBS Benachrichtigung - Ihre Internet-Banking gesperrt	ansehen
UBS AG (info@kuty.sk)	UBS Benachrichtigung - Ihre Internet-Banking gesperrt	ansehen
UBS AG (sport@povecernik.sk) (ozelkalem@manas.edu.kg) (encingerova@ensa.sk)	UBS Benachrichtigung - Ihre Internet-Banking gesperrt	ansehen
UBS Bank AG (mailto:infodesk@ubs.ch)	UBS: Klantenservice.	ansehen
UBS Bank AG (infodesk@ubs.ch)	UBS E-Banking Services Update.	ansehen
UBS Online E-banking (hegedus@mukki.richem.hu) (wilde@almos.vein.hu)	-	ansehen
UNITED NATIONS (BankNoooN00111@siren.ocn.ne.jp)	YOUR VISA-MASTER CARD	ansehen
Visa Abteilung Sicherheit (info@visa-europe.ch)	Bitte lesen Sie sofort!	ansehen
"www.visaeurope.ch" (admin@bournemouthopenbowls.com)	Ihre Karte wird Suspendiert!	ansehen
www.visaeurope.ch (support@visaeurope.ch)	Dringend - Ihre Karte wird Suspendiert!	ansehen
Viseca Card Services (do_not_replay@viseca.com)	Schützen Sie Ihre Kreditkarte	ansehen