digitalcourage Hochschulgruppe

Digitale Selbstverteidigung:

Password Leaks und Account Hacks verhindern

Der Verein und die Hochschulgruppe stellen ihr Engagement und Aktivitäten vor

Digitalcourage e. V.

- Gemeinnütziger Verein für Datenschutz und Bürgerrechte
  - „Für eine lebenswerte Welt im digitalen Zeitalter“
  - BigBrotherAwards
  - Aktionen zu aktuellen Themen
- Digitalcourage-Hochschulgruppe ***(www.digitalcourage.de/hsg-bt)***
  - Vorträge
  - Workshops
  - Lesungen gegen Überwachung
  - BigBrotherAwards Live Stream *(08.06.2019, 18 Uhr im Glashaus)*

Durch Digitalkompetenz können wir uns proaktiv gegen Datendiebstahl schützen

Digitalcourage e. V.

Eine Waffe namens Doxing

Das Sammeln persönlicher Informationen, genannt Doxing, ist ein beliebtes Mittel der Einschüchterung. Das bekommen nun deutsche Politiker und Prominente zu spüren.

Von **Eike Kühl**

7. Januar 2019, 17:03 Uhr / 125 Kommentare

Je mehr Daten wir im Netz verbreiten, desto mehr Daten lassen sich auch über uns sammeln. © Westend61/Getty Images

INHALT

Es geht um private Telefonnummern, Anschriften, E-Mail-Adressen, Dokumente, Bilder und Chatverläufe: Fast 1.000 deutsche Politikerinnen und Politiker, Prominente und YouTuber erleben derzeit, wie es sich anfühlt, im Internet bloßgestellt zu werden. Wie es ist, wenn Informationen an die Öffentlichkeit geraten, die privat bleiben sollten. Und wie schwierig es ist, sowohl gegen die verantwortlichen Personen als auch die Verbreitung vorzugehen.

NETZPOLITIK.ORG

Defensive Strategie und Aufbau von Digitalkompetenz nötig

Überhaupt schwächt staatliches Hacking die IT-Sicherheit für alle Bürger. Dies zeigt der Einsatz von Staatstrojanern. Diese Maßnahme wurde in den letzten Jahren auf Bundesebene und in vielen Bundesländern eingeführt. Für den Einsatz von Staatstrojanern benötigt man Sicherheitslücken in Computerprogrammen. Wird der Staat zum Hacker, der seine Staatstrojaner nutzen will, hat er plötzlich ein Interesse, dass diese Sicherheitslücken offen bleiben. Dafür muss er sie selbst finden oder auf dem Schwarzmarkt einkaufen. Staatstrojaner und Online-Durchsuchungen sind also nicht nur aus bürgerrechtlicher Sicht eine Bedrohung, sondern auch für die Datensicherheit aller.

Weit sinnvoller als staatliches Hacking ist eine breit angelegte Kampagne zur Verbesserung der Datensicherheit. Neben einer personellen Stärkung der Datenschutzbehörden könnte digitale Kompetenz unterschiedlichster Zielgruppen gefördert werden, damit diese lernen, wie sie sich besser schützen. Dabei ist Datensicherheit nur ein kleiner Teil der zu vermittelnden Digitalkompetenz.

Agenda

- Updates
- Mail-Konto
- Passwörter
- Zwei-Faktor-Authentifizierung
- Werbeblocker
- Phishing erkennen und handeln
- GM V20.19

Updates sind unerlässlich

Updates

- Betriebssystem und Software immer aktuell halten, Updates NICHT aufschieben
- Vorher unbedingt wichtige Daten sichern
- Kein Backup? Kein Mitleid!

Agenda

- Updates
- Mail-Konto
- Passwörter
- Zwei-Faktor-Authentifizierung
- Werbeblocker
- Phishing erkennen und handeln
- GM V20.19

Klassische/kostenfreie Mail-Anbieter sollten vermieden werden

Mail-Konto

- Auslesen von Mails
- Speichern, Verarbeiten und Tracken von Daten

- Werbung auf Startseite
- Werbung im Konto
- Werbung in App

Klassische/kostenfreie Mail-Anbieter sollten vermieden werden

Mail-Konto

- Wenn etwas nichts kostet, bist DU das Produkt
- Vertrauenswürdige Anbieter aus Europa nutzen
- Empfehlung in DE:
  - mailbox.org
  - posteo.de

Aliase bieten – sinnvoll verwendet – einen effektiven Schutz

Mail-Konto

- Mindestens fünf Mail-Adressen verwenden
  - Uni ✓
  - Privat ✓
  - Sonstige Registrierungen
  - Dienste mit Geld
  - Jobs (doppeldeutig)
- Aliase nutzen
- Für einmaligen Gebrauch Wegwerf-Mail-Adressen nutzen

Aliase bieten – sinnvoll verwendet – einen effektiven Schutz

Mail-Konto

- *Warum?* SPAM/Phishing
- Weiterer Vorteil: Sortierung per Filter in Ordner
- Namen und (Geburts-)Daten in Mail-Adresse vermeiden

Beim Verfassen von E-Mails und bei der Registrierung per Mail-Adresse kann man effektiv vorbeugen

Mail-Konto

- Haupt-Konto NIEMALS für einen Dienst oder für Mails benutzen
- „Single Sign-on“ vermeiden (Bündelung)
- Empfängerkreis in BCC
- Mail-Adressen nicht streuen
- Text- statt HTML-Format wählen

Agenda

- Updates
- Mail-Konto
- Passwörter
- Zwei-Faktor-Authentifizierung
- Werbeblocker
- Phishing erkennen und handeln
- GM V20.19

Die Berichte zu gestohlenen Zugangsdaten reißen nicht ab

Passwörter

Protokoll zum Daten-GAU

Cyber-Gangster kapern 18 Millionen Mail-Adressen samt Passwörtern

Aktualisiert am Donnerstag, 03.04.2014, 18:47

Im Internet lassen sich viele Daten ausspähen Colourbox

Es ist der zweite schwere Fall von Cyberkriminalität innerhalb kurzer Zeit: Hacker haben 18 Millionen E-Mail-Konten mit den dazugehörigen Passwörtern gestohlen. Die Staatsanwaltschaft Verden stieß auf den gigantischen Datensatz. FOCUS Online liefert alle News zum Daten-GAU.

+++ 18 Millionen Konten betroffen +++

25.01.2019 12:51 Uhr | Security

Neue Passwort-Leaks: Insgesamt 2,2 Milliarden Accounts betroffen

Nach der Passwort-Sammlung Collection #1 kursieren nun auch die riesigen Collections #2-5 im Netz. So überprüfen Sie, ob Ihre Accounts betroffen sind.

Von Ronald Eikenberg

Es gibt sinnvolle Grundsätze zum Umgang mit Passwörtern

Passwörter

- bei jedem Dienst ein Anderes
- Regelmäßiges Ändern ist Unfug
- Ein starkes Passwort ist besser, als ein wechselndes/aufgeschriebenes
- Geräte sperren (Handy, Tablet, PC)
- Sensible Apps zusätzlich sperren

Zunehmende Zeichen-Komplexität bei Passwörtern erschwert das Knacken

- Folgende Möglichkeiten bei nur Zahlen
  - 1 Stelle: _ 10 Möglichkeiten (0-9)
  - 2 Stellen: _ _ 100 Möglichkeiten (0-99)
  - 3 Stellen: _ _ _ 1000 Möglichkeiten (0-999)
  - usw.

Komplexe, aber kurze Passwörter lassen sich schnell knacken

Passwörter

Passwortlänge	maximale Dauer
4	5 Millisekunden
5	464 Millisekunden
6	39 Sekunden
7	54 Minuten
8	3 Tage
9	8 Monate
10	61 Jahre
11	5176 Jahre
12	0,4 Mio. Jahre
13	36 Mio. Jahre

Quelle: BAköV

Annahme: 84 mögliche Zeichen, 9 Mrd. Hashes/Sekunde (NTLM)

Folgende Kriterien (müssen/) sollten bei der Passwort-Wahl berücksichtigt werden

Passwörter

- Mindestlänge: 14 oder mehr Zeichen
- Klein- und Großbuchstaben
- Zahlen
- Interpunktions- und Sonderzeichen

Folgende Kriterien (müssen/) sollten bei der Passwort-Wahl berücksichtigt werden

Passwörter

- keine Wörter, die in Wörterbüchern stehen
- keine Zeichenfolgen auf der Tastatur
- keine ABC- und Zahlenreihen
- keine aufeinanderfolgende Wiederholung

Wer fühlt sich jetzt überfordert?

Passwort-Sätze liefern (/erfüllen alle Kriterien für) „gute“ Passwörter

Passwörter

- Eigene ~~Passwort-Sätze~~ Passphrasen:
  Merken und Variieren wird zum Kinderspiel – versprochen!

- Alternativ Passwortmanager
  - HashiCorp Vault
  - KeePass (vom BSI empfohlen)
  - Auf jeden Fall: FOSS (Free and Open Source Software)

Sichere Passphrasen kann sich jeder merken

Passwörter

- Workshop: Wir erstellen nun „gemeinsam“ sichere Passphrasen
  - *Zettel und Stifte durchgeben*
- Satz-Beispiele:
  - Über 7 Brücken
  - Erholung pur
  - Meine Oma fährt Motorrad

Liedtexte sind für Passwort-Sätze besonders gut geeignet

Passwörter

- PM-U:7Bmdg,7dJu:
  - Peter Maffay: Über 7 Brücken musst du gehn, 7 dunkle Jahre überstehn
- Ep:aS1GtiRg!
  - Erholung pur: auf Sardinien 1 Glas trockenen italienischen Rotwein genießen!
- M0f1HM-ubbe!
  - Meine Oma fährt im Hühnerstall Motorrad-und bietet bei ebay!
    und lernt in der Bib!
    und bestellt per Amazon!

Agenda

- Updates
- Mail-Konto
- Passwörter
- Zwei-Faktor-Authentifizierung
- Werbeblocker
- Phishing erkennen und handeln
- GM V20.19

Ein zweiter Faktor hebt den Konten-Schutz auf die nächste Stufe

2FA

- Warum zweiten Faktor hinzufügen? Macht das nicht mehr Arbeit?
  - Wissen + Besitz
  - Wenig Mehraufwand aber viel mehr Sicherheit
- Kein echter zweiter Faktor: SMS → von BSI nicht empfohlen
- Weicher zweiter Faktor: Authenticator App
- Harter zweiter Faktor: Hardware Token (ähnlich EC-Karte oder als Token)

Ein zweiter Faktor hebt den Konten-Schutz auf die nächste Stufe

2FA

- Welche Dienste unterstützen welche Methode?
  - SMS/Code bietet quasi jeder Dienst
  - Hardware Token werden immer beliebter
- Twofactorauth.org
- Selbst getestet: PayPal, facebook, amazon, XING, mailbox.org, Twitter

Wir aktivieren nun gemeinsam einen zweiten Faktor

2FA

- Workshop: Wir erstellen nun „gemeinsam“ einen zweiten Faktor
- Authenticator App (installieren und starten)
  - Empfehlung: andOTP – Android OTP Authenticator
  - Passwort festlegen
- Dienst eurer Wahl aufrufen (Mail, Geld und Netzwerke sehr sensibel)
- Einstellungen auswählen
  - 2-Faktor-Anmeldung o. ä.
  - Code scannen mit andOTP, Code in Dienst eingeben und bestätigen

Agenda

- Updates
- Mail-Konto
- Passwörter
- Zwei-Faktor-Authentifizierung
- Werbeblocker
- Phishing erkennen und handeln
- GM V20.19

Werbung ist nicht nur nervig

Werbeblocker

- Notwendigkeit: Nicht nur nervig, sondern auch Datensammlung und Verteilung von Malware über Werbenetzwerke

Security › 7-Tage-News › 03/2016 › **Malvertising: Erpressungs-Trojaner über AOL, BBC und MSN verteilt**

UPDATE 16.03.2016 10:46 Uhr | Security

Malvertising-Kampagne: Webseiten von AOL, BBC und MSN verteilten Erpressungs-Trojaner

Verschiedene Sicherheitsforscher warnen, dass populäre Webseiten von etwa AOL, BBC und The New York Times Opfer von manipulierten Werbeanzeigen geworden sind und über diese bereits zehntausende Besucher mit Verschlüsselungs-Trojanern infiziert haben.

Von Dennis Schirrmacher

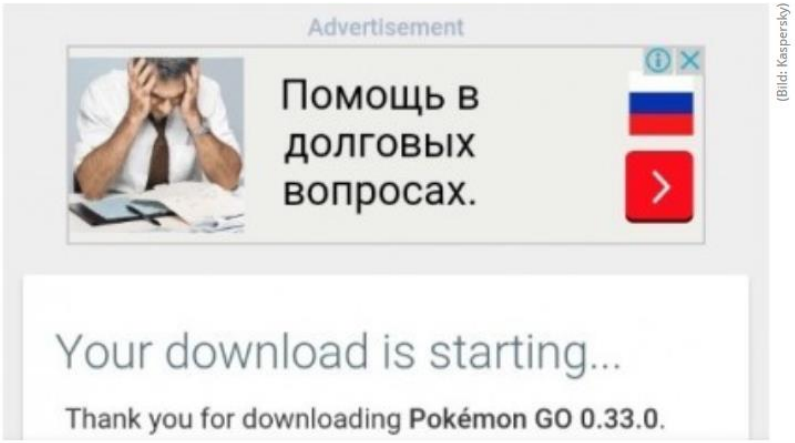
142

ADSENSE

Google entfernt Bankentrojaner aus Werbenetzwerk

Erneut ist über ein Werbenetzwerk Schadsoftware verteilt worden. Eine Google-Adsense-Kampagne hatte versucht, Android-Nutzern einen Bankentrojaner unterzuschieben. Die entsprechenden Anzeigen wurden mittlerweile deaktiviert.

9. November 2016, 17:09 Uhr, Hauke Gierow



(Bild: Kaspersky)

Adsense als Trojaner-Schleuder

Werbung ist nicht nur nervig

Werbeblocker

- Empfehlungen für Browser: **uBlock origin**

- Zusätzlich für Android: **Blokada** (Einsteiger), **NetGuard** (Fortgeschrittene)
- Zusätzlich für iOS: **AdGuard für iOS Pro**

- Hilfe erwünscht? Workshop bei Vortrag „Browser und Mail Client härten“

Agenda

- Updates
- Mail-Konto
- Passwörter
- Zwei-Faktor-Authentifizierung
- Werbeblocker
- Phishing erkennen und handeln
- GM V20.19

Jeder ist ein interessantes Phishing-Opfer

- Phishing-Angriffe als zweitgrößte Gefahr nach Erpressungstrojanern
- Für Betrüger vor allem alles mit **Geld** (Amazon, PayPal, Online Banking, eBay,…), **sensiblen Daten** (Nackedei-Bilder in der Cloud,…) sowie **Mail-Konten** interessant
- Phishing Mails immer professioneller, sehen täuschend echt aus

Spear Phishing ist eine spezialisierte Form

Phishing: erkennen und handeln

Ein sorgloser Klick auf Links in der Timeline kann sehr teuer werden.
(Foto: imago/Ikon Images)

Freitag, 02. Juni 2017

Sie liefern selbst die Infos

Viele Facebook-Nutzer Spear-Phishing-Opfer

Hacker greifen Facebook-Nutzer vermehrt über deren Timeline an. Viele fallen darauf rein, weil die Methode der Gangster besonders raffiniert und persönlich ist.

Teilen Twittern Teilen

Hacker starten ihre lukrativsten Angriffe zunehmend über getarnte Beiträge in sozialen Netzwerken - und sehr viele Nutzer fallen darauf rein. Die Gangster legen ihre Opfer via "Spear Phishing" herein, das wesentlich raffinierter als das herkömmliche Phishing ist.

heise online ⟩ News ⟩ 04/2019 ⟩ **Mysteriöse Datenbank mit Daten von Millionen US-Bürgern ungeschützt…**

29.04.2019 18:27 Uhr

Mysteriöse Datenbank mit Daten von Millionen US-Bürgern ungeschützt im Netz

Sensible Daten von 80 Millionen US-Haushalten liegen in einer offen zugänglichen Datenbank. Der Besitzer konnte bisher nicht ermittelt werden.

Von **Oliver Bünte** 146

"Goldgrube" für Identitätsdiebe

Nach Ansicht der Sicherheitsforscher von *vpnMentor* sei diese Datenbank aufgrund ihres Umfangs und der enthaltenen Detailinformationen einzigartig und damit "eine Goldgrube für Identitätsdiebe und andere Angreifer" sei. Sie könnten mit diesen Daten leicht die E-Mail-Adressen ermitteln und mit frei verfügbaren Daten aus dem Web wie beispielsweise aus sozialen Medien verknüpfen. Damit könnten nach Alter und Einkommen gezielt Personen identifiziert und beispielsweise per Telefon oder Phishing-E-Mail angegriffen, weitere Daten ermittelt und damit deren Identität genutzt werden.

Anhand von sechs Merkmalen kann man viele Phishing Mails identifizieren

Von: PayPal [mailto:service@paypal-deutschland.de]
Gesendet: Donnerstag, 19. Dezember 2013 04:14
Betreff: PayPal-Mitteilung
Anhang: komplexe.pdf

Guten Tag,

leider haben wir in letzter Zeit Zugriffsversuche von Dritten auf Ihr Konto festgestellt. Zu Ihrer Sicherheit haben wir Ihr Konto vorerst eingeschränkt.

Wir bitten Sie, Ihre Identität unter folgendem Link zu bestätigen.

PayPal - Verifikation

ACHTUNG! Sollten Sie Ihre Identität nicht zeitnah bestätigen, wird Ihr Konto samt möglichem Guthaben dauerhaft gesperrt!

Mit freundlichen Grüßen,

PayPal

Anhand von sechs Merkmalen kann man viele Phishing Mails identifizieren

Phishing: erkennen und handeln

Von: PayPal [mailto:service@paypal-deutschland.de]
Gesendet: Donnerstag, 19. Dezember 2013 04:14
Betreff: PayPal-Mitteilung
Anhang: komplexe.pdf

Guten Tag,

leider haben wir in letzter Zeit Zugriffsversuche von Dritten auf Ihr Konto festgestellt. Zu Ihrer Sicherheit haben wir Ihr Konto vorerst eingeschränkt.

Wir bitten Sie, Ihre Identität unter folgendem Link zu bestätigen.

PayPal - Verifikation

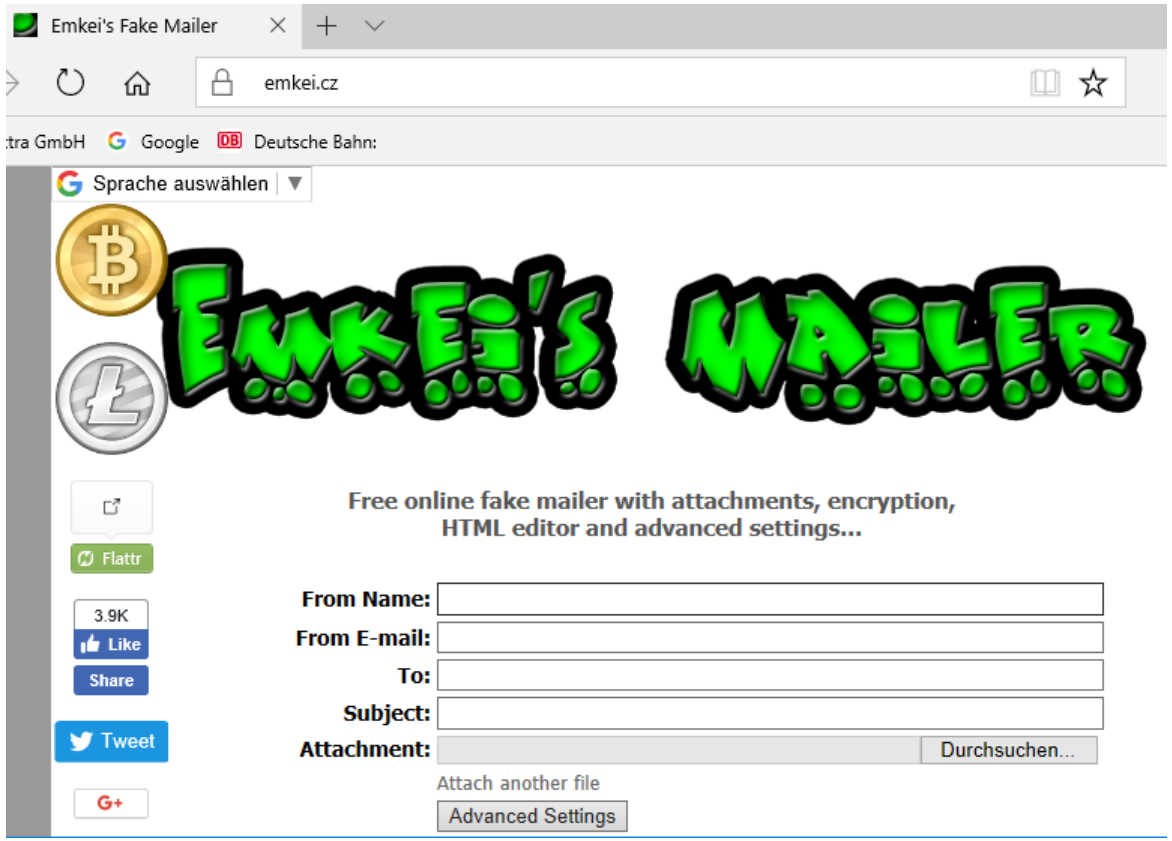
ACHTUNG! Sollten Sie Ihre Identität nicht zeitnah bestätigen, wird Ihr Konto samt möglichem Guthaben dauerhaft gesperrt!

Mit freundlichen Grüßen,

PayPal

Absender-Adressen lassen sich sehr leicht fälschen

Phishing: erkennen und handeln



Anhand von sechs Merkmalen kann man viele Phishing Mails identifizieren

Phishing: erkennen und handeln

Von: PayPal [mailto:service@paypal-deutschland.de]
Gesendet: Donnerstag, 19. Dezember 2013 04:14
Betreff: PayPal-Mitteilung
Anhang: komplexe.pdf

Guten Tag,

leider haben wir in letzter Zeit Zugriffsversuche von Dritten auf Ihr Konto festgestellt. Zu Ihrer Sicherheit haben wir Ihr Konto vorerst eingeschränkt.

Wir bitten Sie, Ihre Identität unter folgendem Link zu bestätigen.

PayPal - Verifikation

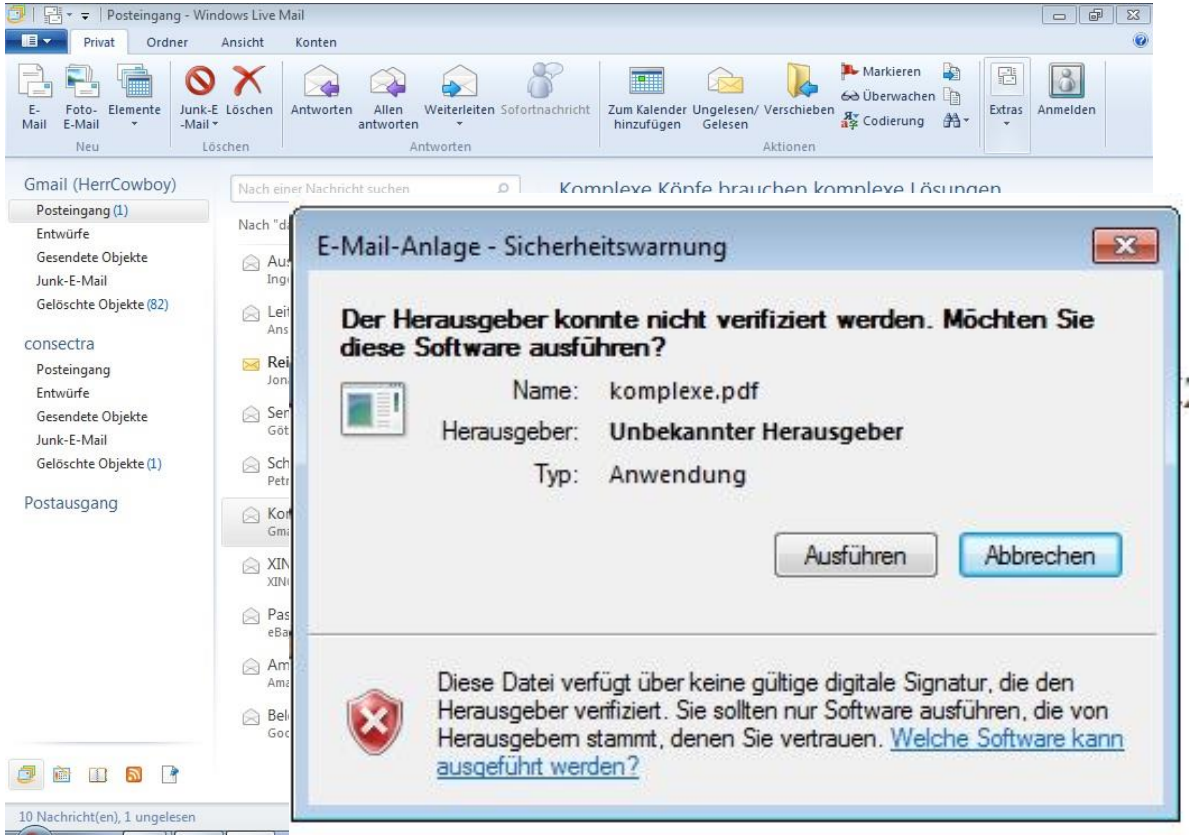
ACHTUNG! Sollten Sie Ihre Identität nicht zeitnah bestätigen, wird Ihr Konto samt möglichem Guthaben dauerhaft gesperrt!

Mit freundlichen Grüßen,

PayPal

.exe-Dateien werden gerne „getarnt“

Phishing: erkennen und handeln



Anhand von sechs Merkmalen kann man viele Phishing Mails identifizieren

Phishing: erkennen und handeln

Von: PayPal [mailto:service@paypal-deutschland.de]
Gesendet: Donnerstag, 19. Dezember 2013 04:14
Betreff: PayPal-Mitteilung
Anhang: komplexe.pdf

Guten Tag,

leider haben wir in letzter Zeit Zugriffsversuche von Dritten auf Ihr Konto festgestellt. Zu Ihrer Sicherheit haben wir Ihr Konto vorerst eingeschränkt.

Wir bitten Sie, Ihre Identität unter folgendem Link zu bestätigen.

PayPal - Verifikation

ACHTUNG! Sollten Sie Ihre Identität nicht zeitnah bestätigen,

http://sicherheit.paypal-deutschland-team.com/D91238101222/V345_34591A_2384723B/security/AX24553435667773/

Mit freundlichen Grüßen,

PayPal

Für den Umgang mit Hyperlinks haben sich folgende Grundsätze bewährt

- Links in Mails immer mit Vorsicht genießen
- URL von rechts nach links lesen
  - *Beispiel: http://campusonline.uni-bayreuth.de.hacker.io/*
- Links nur nutzen, wenn selbst angefordert:
  - Bestätigung nach Anmeldung bei Webseite/Dienst
  - Zurücksetzen des Passwortes
  - Downloadlink einer zuvor bestellten Software
  - Sonst: Lesezeichen verwenden oder selber Seite öffnen

Anhand von sechs Merkmalen kann man viele Phishing Mails identifizieren

Phishing: erkennen und handeln

Von: PayPal [mailto:service@paypal-deutschland.de]
Gesendet: Donnerstag, 19. Dezember 2013 04:14
Betreff: PayPal-Mitteilung
Anhang: komplexe.pdf

Guten Tag,

leider haben wir in letzter Zeit Zugriffsversuche von Dritten auf Ihr Konto festgestellt. Zu Ihrer Sicherheit haben wir Ihr Konto vorerst eingeschränkt.

Wir bitten Sie, Ihre Identität unter folgendem Link zu bestätigen.

PayPal - Verifikation

ACHTUNG! Sollten Sie Ihre Identität nicht zeitnah bestätigen,

Mit freundlichen Grüßen,

PayPal

http://sicherheit.paypal-deutschland-team.com/D91238101222/V345_34591A_2384723B/security/AX24553435667773/

Anhand von sechs Merkmalen kann man viele Phishing Mails identifizieren

Phishing: erkennen und handeln

Wichtige Information: Wir haben verdächtige Kontobewegungen festgestellt!

Von: Amazon <mailer@2ck42.science>
An: [redacted]
Datum: 11.09.2017 05:39:07

amazon.de

Wichtige Information! - Überprüfung erforderlich
Datum: 11.09.2017

Guten Tag,

wir haben einen verdäch ch in Ihrem Amazon-Konto (raimondkiess@web.de) festgestellt,
welcher nicht von Ihrem E gerät unternommen wurde. Zum Schutze Ihrer persönlichen Daten, wurde der Zugriff auf Ihr Amazon-Konto vorübergehend eingeschränkt.

Wir bitten Sie daher Ihre hinterlegten Daten zu bestätigen, sollten Sie dieser E-Mail . nicht innerhalb von 48 Stunden nach kommen müssen wir Ihr Nutzerkonto aufgrund von Datenschutzgründen sperren.

Weiter zur Überprüfung

Wir freuen uns auf Ihren näc n Besuch!
Amazon.de

Dies ist eine automat Nachricht. Bitte antworten Sie nicht auf dieses Schreiben.
Wenn Sie eine Frage n Sie sich bitte an unseren Kundendienst.

© 1998-2017, Amazon.de, Inc. oder Tochtergesellschaften
Umsatzsteueridentifikationsnummer: LU 20260743 Amazon EU société à responsabilité limitée, 5 rue Plaetis, L-2338 Luxemburg

PayPal

Donnerstag, 16. November 2017 (MEZ)
Bearbeitungsnummer: E7163075643A14E5

Wichtige Information

Sehr geehrter Kunde,

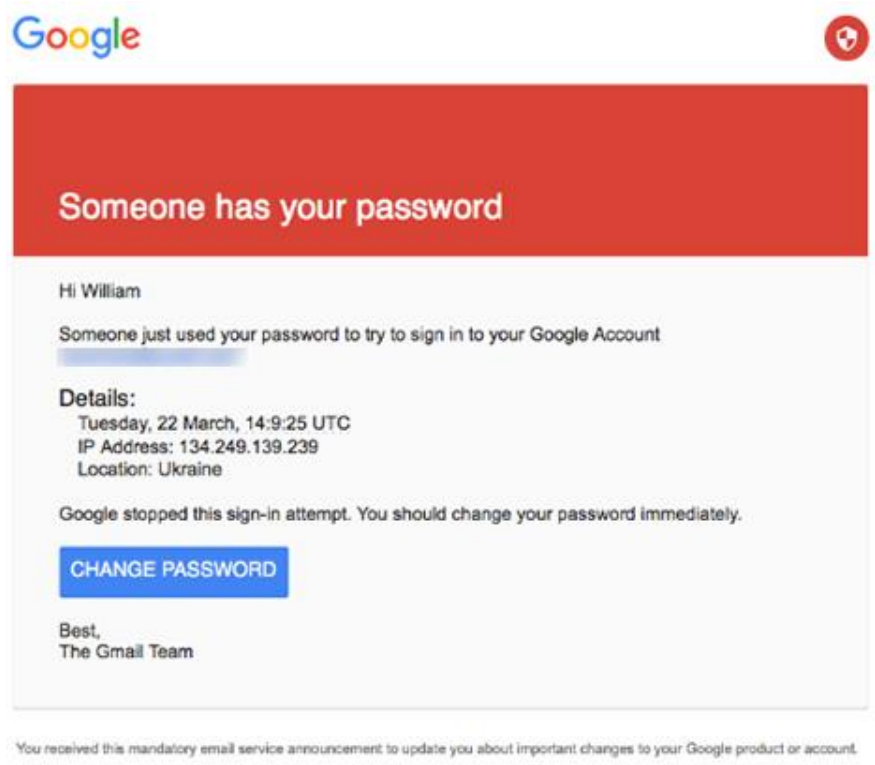
Aufgrund einer Eu-Gesetzesregelung sind alle Zahlunsanbieter im Europäischen Raum seit dem 05.11.2017 gesetzlich dazu verpflichtet Ihre Kundendaten zu verifizieren.

Aus diesem Grund müssen wir Sie bitten Ihre Kundendaten zu bestätigen. Bitte nehmen Sie sich 5 Minuten Zeit und führen Sie den Prozess unter folgendem Link durch:

Bestätigungsprozess starten

Was mache ich jetzt?

Bitte bestätigen Sie Ihre Daten innerhalb von 48 Stunden. Sollte keine Bestätigung vorliegen sind wir dazu gezwungen Ihr Konto vorübergehend zu deaktivieren.



Google

Someone has your password

Hi William

Someone just used your password to try to sign in to your Google Account [redacted]

Details:
Tuesday, 22 March, 14:9:25 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

CHANGE PASSWORD

Best,
The Gmail Team

You received this mandatory email service announcement to update you about important changes to your Google product or account.

E-Mails sollten immer überprüft werden

Phishing: erkennen und handeln

- Plausibilität der Mail überprüfen
- Absender prüfen, im Zweifel anrufen
- Anhänge mit Vorsicht genießen
- Vorsicht bei Links → „mouse over“

Für den Fall der Fälle hilft die folgende Anleitung

Phishing: erkennen und handeln

- Ruhe bewahren

- WLAN aus-/Flugmodus anschalten
- Fehlermeldungen nicht wegklicken (ideal: zusätzlich Screenshot speichern)
- Nicht ausschalten/neustarten

- Bei Verdacht: IT-Servicezentrum aufsuchen („Anlaufstelle“)
- Kommiliton.innen warnen, falls Datenaustausch mit infiziertem Rechner stattfand

Agenda

- Updates
- Mail-Konto
- Passwörter
- Zwei-Faktor-Authentifizierung
- Werbeblocker
- Phishing erkennen und handeln
- GM V20.19

Der gesunde Menschenverstand sollte nicht unterschätzt werden

GM V20.19

- **GM V20.19** ist kostenlos!!11!!!1

Belege, Beispiele und weiterführende Erläuterungen findet ihr auf einigen Webseiten

Weiterführende Links

- Digitalcourage.de/digitale-selbstverteidigung
- Kuketz-blog.de/einstiegshilfe
- Privacy-handbuch.de/print.htm
- Mobil-sicher.de/themen/kategorie/basissicherung