Dieses Dokument ist nur für Mitglieder vom Global Citizen Explorer. Eine Weiterreichung der Inhalte wird von den Autoren strafrechtlich geahndet.

Die Inhalte dieses Dokuments leisten keine rechtliche, steuerliche oder Investment-Beratung. Nichts sollte als solches aufgefasst werden!

Rechts- und Nutzungsvereinbarung

Sämtliche durch GlobalCitizenExplorer.com (folgend auch GCE genannt) auf seiner Webseite oder in Dokumenten zur Verfügung gestellten Inhalte dienen lediglich der Information des Nutzers. GCE, Autor / Herausgeber, ist stets bemüht, die dargestellten Informationsangebote mit Sorgfalt zu erstellen.

GCE übernimmt jedoch ausdrücklich keine Gewähr oder gar Haftung hinsichtlich der Richtigkeit, Vollständigkeit, Aktualität oder auch Verfügbarkeit. Sämtliche Inhalte stellen weder eine individuelle Empfehlung dar, noch sind Inhalte und Darstellungen als Einladung / Aufforderung / Angebot zur Handlung, Unterlassung, zum Kauf oder Verkauf zu verstehen.

Alle Informationsangebote und Darstellungen in diesem Dokument und/oder auf der Webseite sind ausschließlich auf eine selbständige und unabhängige Entscheidung des Lesers orientiert und ersetzen nicht eine juristische bzw. steuerrechtliche Beratung.

GCE weißt Sie ausdrücklich darauf hin, dass auch im Ausland erwirtschaftete Erträge in Ihrem Heimatland der Steuerpflicht unterliegen können. GCE übernimmt diesbezüglich keine Rechts- und Steuerberatung.

Für die Erfüllung aller in- und ausländischen Steuerpflichten sind ausschließlich Sie verantwortlich. Bitte lassen Sie sich hinsichtlich ggf. bestehender Steuerpflichten durch einen Steuerberater oder auch Rechtsanwalt Ihres Vertrauens beraten.

Es gelten unsere Rechts- und Nutzungshinweise, unsere Legal Details, welche Sie bereits durch Nutzung dieses Dokuments und/oder unserer Webseite verbindlich anerkennen.

Herausgeber

Fuckdsgvo Limited
P.O. Box 1405
Majuro
Marshall Islands

Kontakt: support@globalcitizenexplorer.com

Inhaltsverzeichnis

Das Internet weiß alles und vergisst nichts!

Jeden Tag fütterst Du das Internet mit Informationen, die für oder gegen Dich verwendet werden können. Dein Handy erkennt Dein Umfeld, Deine Gespräche und Deine Termine.

Dein Fitnessarmband weiß ob Du gesund bist, Du Dich viel bewegst, Du über- oder untergewichtig bist. Instagram und Snapchat wissen wo Du bist, welche Fotos Du gut findest und auch gerne mit deinen Freunden teilst.

Netflix kennt Deine Lieblingsserien und Filme. Amazon kennt Deinen Modegeschmack und sogar den Inhalt Deines Kühlschrankes.

Die Aussage, dass das Internet „alles" weiß ist nicht ganz richtig, jedoch trotzdem recht akkurat.

Wir leben in einer Gesellschaft, in der man alles mit Apps aufzeichnen, planen und bearbeiten kann.

Wir können Türen öffnen ohne anwesend zu sein, den Inhalt unseres Kühlschrankes kontrollieren und automatisch neue Lebensmittel über Amazon bestellen lassen.

Das Internet bietet viele großartige - auch vermeintlich kostenlose - Möglichkeiten. Schließlich ermöglicht dieses uns vom GCE und vielen anderen Menschen einen ortsunabhängigen Lebensstil.

Doch mit der Sammlung von Echtzeit-Daten und deren Analyse bezahlst auch Du einen gewissen Preis: Je mehr Du das Internet mit Informationen fütterst, desto transparenter wird Dein digitales Ich und Dein reales Leben - das macht Dich berechenbar und sogar angreifbar.

Diese Berechenbarkeit raubt uns einen Teil unserer Freiheit.

Daher werden wir Dir in dieser Anleitung dabei helfen die Balance zwischen Bequemlichkeit und Sicherheit zu finden.

Wir werden Dir die neusten Entwicklungen in Punkto Datensicherheit und Hacking näherbringen.

Zudem werden wir Dir zeigen gegen welche Risiken sich Windows-, Mac-, Android- und iPhone-Nutzer schützen sollten.

Selbstverständlich werden wir Techniken, Programme und Apps vorstellen, die wir selber nutzen, um uns dem Fadenkreuz von Hackern und staatlicher wie privatwirtschaftlicher Massenüberwachung zu entziehen.

Durch die Anwendung unserer Strategien machst Du Dich weniger attraktiv für Verbrecher und Datensammler.

Wir können keine Unantastbarkeit versprechen. Wenn ein Hacker die nötigen Mittel hat, dann wird er einen Weg an Deine Daten finden.

Wenn Du Ziel der Regierung wirst, werden deren Geheimdienste ebenfalls einen Weg finden. Deine Aufgabe ist es hier ihnen den Weg so schwer wie nur irgend möglich zu machen.

Es ist wie mit einem Auto, die Alarmanlage, Lenkradsperre und das GPS-Tracking werden einen engagierten Dieb nicht stoppen, jedoch wirst Du mit einer Kombination aus all dem nicht so wahrscheinlich zum Ziel der Täter werden.

Und genau dieses Prinzip wenden wir zum Schutz Deiner digitalen Identität an.

Vermeidungsstrategien gegen Hackerangriffe

Es gibt unzählbar viele Arten und Weisen wie ein Hacker an Deine Daten gelangen kann. In diesem Kapitel stellen wir Dir eine sehr gängige Art vor, deren Ziel jeder von uns schon mindestens einmal wurde.

Phishing

Phishing ist eine Methode, bei der Du dazu gebracht wirst sensible Daten unbewusst an Angreifer abzugeben.

Solche Angreifer arbeiten im Normalfall mit E-Mails, welche Dich dazu auffordern beispielsweise Dein Konto zu verifizieren oder Dich wegen eines Problems erneut einzuloggen.

Solltest Du auf den angebotenen Link klicken, wirst Du auf eine Dummy-Seite weitergeleitet, welche einer legitimen nahezu identisch sieht.

Solltest Du hier Dein Passwort eingeben, so wird es im Hintergrund als Klartext gespeichert. Somit erlangen die Hacker Dein Passwort und können auf Dein Profil zugreifen.

Du wirst nach der „Bestätigung" normalerweise auf die Originalseite (z.B. Google, Amazon, Facebook,...) weitergeleitet, wodurch Du den Betrug meist erst merkst, wenn es zu spät ist.

So erkennst und vermeidest Du Phishing

Untersuche die E-Mail

Wenn Du eine E-Mail erhältst, die Dich zum Login auffordert, untersuche sie auf irgendetwas verdächtiges.

Ist der Absender korrekt?

Die meisten Betrüger nutzen E-Mail-Adressen, die der richtigen sehr ähnlich sehen.

Beispiel:

original: @yahoo-inc.com
phishing: @yahooo.com

Die meisten Leute wissen nicht, dass Yahoo-Mails immer von yahoo-inc.com sind, daher sähe eine Adresse wie info@yahooo.com legitim aus.

Um ein besseres Bild von Phishing-Mails zu erhalten, kannst Du auch einfach in Deinen Spam-Ordner schauen.

Die ähnlichsten Adressen sind meist schon vergeben, daher wirken die meisten Spam-Mail-Adressen sehr illegitim.

Ist die E-Mail personalisiert?

Die meisten Unternehmen/Webseiten personalisieren ihre E-Mail soweit, dass Dein Name und/oder Benutzername genannt wird.

Bei Phishing-Mails wird die Anrede meist sehr unpersönlich formuliert, wie „Hallo Nutzer/in" oder „Liebe/r Kunde/in".

Sollte dies der Fall sein, dann solltest Du einen zweiten Blick wagen und kontrollieren, ob es sich um eine legitime Nachricht handelt.

Wie sieht die E-Mail aus?

Die meisten Unternehmen verwenden in all ihren E-Mails stets eine standardisierte Struktur.

Diese Strukturen sind es, welche bei Phishing-Mails oft nicht stimmen. Sei es ein ähnliches, aber doch anderes Logo oder die falsche Platzierung von bestimmten Angaben.

Auch kommt es öfter vor, dass solche Phishing-Mails zweisprachig verfasst sind. Damit meinen wir, dass ein Satz beispielsweise Englisch und Deutsch enthält, da die Mail unachtsam per Programm erstellt wurde.

Solche Unstimmigkeiten solltest Du ebenfalls beachten.

Wirst Du zur Aktion "gedrängt"?

Der Verfasser einer Phishing-Mail möchte Dich dazu bringen, dass Du die angegebenen Links klickst und Deine Daten einträgst.

Dieser Antrieb wird meist schnell klar, da Du regelrecht dazu gedrängt wirst Deine Daten einzugeben.

Sei es ein Befehl, ein rotes und auffälliges Banner oder sonstige Besonderheiten, die Dir aufdringlich erscheinen.

Falls Du eine solche E-Mail erkennst, dann markiere diese auch als Spam.

Wenn genug Leute diesen Absender als Spam markieren, dann handeln die meisten Anbieter, indem die Mails des betrügerischen Absenders automatisch in den Spam-Ordner geleitet werden.

Überprüfe die Webseite

Überprüfe die URL-Adresse, bevor Du den Link zur Seite nutzt. Das kannst Du ganz einfach über eine Google-Suche prüfen, da dort normalerweise auf der ersten Seite keine Phishing-Pages angezeigt werden.

Die häufigsten Änderungen der URL sind übliche Rechtschreibfehler, extra Buchstaben oder eine andere Domain (z.B. „.com" statt „.net").

Wenn Du auch nach all diesen Tests noch nicht von der Echtheit der Seite überzeugt bist, dann nutze einfach den eben schon vorgeschlagenen Weg über Google oder andere Suchmaschinen.

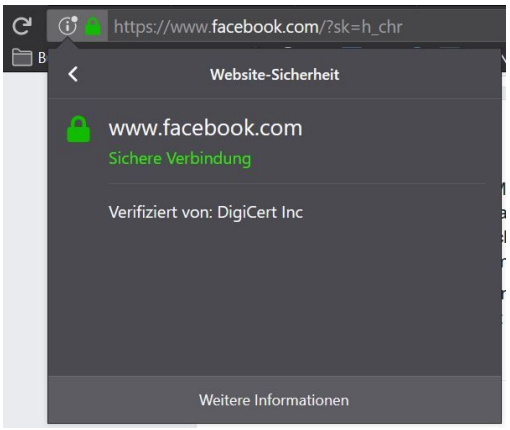
Es gibt Fälle von Phishing, bei denen es sogar schon ausreicht, durch das Klicken des Links Malware zu installieren. Also nimm Dir am besten diese Faustregel zu Herzen: Klicke nie auf einen Link, dessen Echtheit zweifelhaft ist.

Ist die Webseite verschlüsselt?

Überprüfe, ob die URL eine „https://" ist oder eine „http://", um sicher zu gehen, dass die Seite über das SSL-Protokoll verschlüsselt ist.

Zudem wird bei einer „https://" in der Suchleiste ein Schloss-Symbol angezeigt, welches Dir zeigt, dass die besuchte Seite korrekt verschlüsselt ist.

Das Symbol muss links in der Suchleiste und nicht irgendwo auf der Seite selber eingeblendet sein. Nur das Symbol in der Suchleiste zeigt die Verschlüsselung zuverlässig an.



Wenn Du auf das Symbol klickst, erhältst Du Informationen über diese Seite und Du kannst Dir das SSL-Zertifikat anzeigen lassen.

Falls Du keinerlei Informationen über diese Seite erhältst oder Fehlermeldungen angezeigt werden und das SSL-Zertifikat nicht angezeigt werden kann bzw. dieses bereits abgelaufen sein sollte, dann ist die Legitimität dieser Webseite unsicher.

Die Basis Deiner Sicherheit: Passwörter

Jeder weiß, dass gute Passwörter wichtig sind. Ganz egal, ob es sich um das Passwort zu Deiner E-Mail handelt oder Deinem Kundenkonto bei H&M.

Aber um die Wichtigkeit Deiner Passwörter zu verdeutlichen, stelle Dir einfach ein Haus vor. Du kannst Gitter haben, Alarmanlagen und auch Sicherheitskameras. Das alles bringt aber rein gar nichts, wenn Deine Türen nicht ordentlich verschlossen sind.

So verhält es sich auch mit Deinem Computer. Alle Sicherheitsmaßnahmen helfen nichts, wenn die Basis schwach ist.

Also stelle ich Dir folgende Frage: Hast Du wirklich starke Passwörter?

Wenn Du diese Frage selbstbewusst mit „Ja" beantworten kannst, dann hast Du hier die Chance es zu testen.

Wenn Du diese Frage aber nicht mit „Ja" beantworten kannst oder Du unsicher bist, dann solltest Du in diesem Kapitel Stift und Papier auspacken, um mitzuschreiben.

Wie Hacker Deine Passwörter knacken können

Um ein wirklich sicheres Passwort erstellen zu können, musst Du erst verstehen gegen wen und was Du Dich verteidigen musst, wie sie arbeiten und wo ihre Limits liegen.

Wenn Du das verstanden hast, wird es kinderleicht sein das Risiko eines erfolgreichen Hacker-Angriffes und den möglicherweise entstehenden Schaden zu minimieren - selbst dann, wenn ein Hacker es schafft Dein Passwort zu erlangen.

Hacker können Deine Passwörter auf unzähligen Wegen erlangen, wie zum Beispiel:

- **Phishing:** Sie bringen Dich dazu Dein Passwort auf einer Seite einzugeben, die wie eine vertrauenswürdige Seite aussieht (zum Beispiel Deine Online-Banking-Webseite).
- Sie **infizieren** Deine Geräte mit Malware, die z.B. Deine Tastatur-Aktivitäten aufzeichnen können.
- Sie **hacken** sich in Webseiten und greifen auf deren Mitgliederdaten zu.
- **Brute-Force-Methode**: Sie nutzen ein automatisiertes Programm, dabei werden unterschiedliche Kombinationen aus Benutzernamen und Passwörtern in sekundenschnelle durchgetestet.

Davon abgesehen, dass Du selber Ziel eines Hackers wirst, sind es meistens Zugriffe auf Datenbanken von Webseiten, bei denen Daten gestohlen werden.

Hier sind ein paar der historisch größten Hacks, bei denen Passwörter gestohlen wurden:

- Yahoo 2013: Bei einem Cyberangriff im August 2013 wurden die Konten von knapp einer Milliarde Yahoo-Nutzern kompromittiert.

Dabei wurden Namen, E-Mail-Adressen, Telefonnummern, Geburtsdaten und verschlüsselte Passwörter abgegriffen.

- Sony Playstation Network 2011: Cyberangriff auf das digitale Serviceportal Playstation Network (PSN). Neben einer Ausfallzeit des PSN von knapp vier Wochen (!) wurden bei der Cyberattacke jedoch auch die Daten (Kreditkarteninformationen und persönliche Daten) von rund 77 Millionen PSN-Abonnenten gestohlen.
- Livingsocial.com 2013: Es wurden die Passwörter, E-Mail-Adressen und persönlichen Informationen von circa 50 Millionen Nutzern der E-Commerce-Website gestohlen.
- Adobe Systems 2013: Circa 38 Millionen Datensätze von Adobe-Kunden wurden im Zuge dieses Cyberangriffes gestohlen.

Vorfälle wie diese werden erst nach Jahren bekannt gegeben, denn die Hacker beginnen meist auch erst nach Jahren die erlangten Daten zu verkaufen.

Warum? Weil diese Daten für sie sehr nützlich sein können.

Die meisten Menschen haben eine ganz gewisse Art und Weise, wie sie Passwörter erstellen. Ob es Namen mit Daten sind, oder zufällige Wörter mit zufälligen Zahlen. Eine gewisse Gewohnheit schleicht sich bei den meisten ein, denn Muster erlauben es sich die Passwörter besser zu behalten.

Genau diese Muster sind es auf die Hacker setzen. Sie studieren Dein Passwort und versuchen ein Muster zu erstellen, um auch auf andere Konten Zugriff zu erlangen.

Manchmal sind solche Muster erst gar nicht nötig, da es Menschen gibt, die ein Passwort für mehrere Konten nutzen. Solche Gewohnheiten machen es einem Hacker selbstverständlich sehr leicht.

Aber allein die Analyse der Daten dauert nicht so lange.

Es dauert auch so lange, da die gestohlenen Daten meist erst entschlüsselt werden müssen.

Diese Verschlüsselung kommt daher, da viele Unternehmen und Webseiten-Betreiber die Daten ihrer Kunden zusätzlich vor solchen und anderen Angriffen schützen möchten.

Wenn der Schutz also nicht ausreicht und Daten entwendet werden, dann ist es meist der Fall, dass die Betreiber ihre Kunden benachrichtigen. Ob per Mail oder Anzeige auf der Seite ist egal.

Leider handeln so nicht alle. Es gibt einige Betreiber, die solche Vorfälle geheim halten, damit sie keine „Negativwerbung" haben.

Bei den eben vorgestellten Beispielen handelt es sich um sehr bekannte und viel genutzte Seiten, die viel Geld und Zeit in die Sicherheit der Daten stecken. Trotzdem haben es Hacker geschafft diese Seiten erfolgreich zu hacken.

Was glaubst Du also, wie viele kleine Webseiten täglich gehackt werden und wie viele Daten unbemerkt gestohlen werden?

Verständlicherweise fragst Du Dich jetzt vielleicht, ob auch Deine Daten jemals entwendet wurden. Du musst Dir jetzt nicht Deinen Kopf zerbrechen oder stundenlang auf die Suche nach Vorfällen gehen, welche Dich betreffen.

*Du kannst ganz simpel auf der Webseite > ********** < Deine Mail-Adresse eingeben und erfahren, ob sie von einem bereits aufgedeckten Vorfall betroffen war.*

Sehr interessant ist es auch Deine ehemaligen oder sehr alten Mail-Adressen zu checken, denn wie Du eben erfahren hast dauert es manchmal Jahre bis zur Bekanntgabe.

Du kannst über diese Webseite auch gleich Deine wichtigsten Adressen im Reiter "Notify me" eintragen und bestätigen, damit Du zukünftig sofort über diverse Cyberattacken - die Dich betreffen - informiert wirst.

Im Fall eines Angriffes, versucht ein Hacker wie erwähnt durch Muster oder das gleiche Passwort in andere Konten hineinzukommen. Dort möchte er sensible Daten entwenden und Dir eventuell sogar den Zugriff auf Dein Konto entziehen.

Das Passwort Deiner Mail-Adresse ist also mit eines der wichtigsten und sollte eines der stärksten sein. Sollte ein Hacker sich in Dein E-Mail-Konto hacken können, so kann er alle damit verbundenen Konten übernehmen. Dafür muss er nur auf „Passwort vergessen" klicken und die Bestätigungsmail abfangen.

Anschließend kann er das Passwort und die Mail-Adresse dieses Accounts ändern. Somit hat er vollen Zugriff auf Deine Daten und Du hast keine Chance es rückgängig zu machen.

Nicht immer bist Du das Ziel einer solchen Attacke, manchmal bist Du „nur" der Mittelsmann.

Wir alle wissen, dass man keine Links klicken sollte, deren Legitimität nicht sicher ist. Aber wie sieht es aus bei Links von Freunden, Kollegen und Familienmitgliedern?

Es gibt Angriffe, bei denen Deine Mail-Adresse nur dazu genutzt wird, um anderen zu schaden.

Ein Beispiel wie Passwörter geknackt werden können

Wir haben vorhin erwähnt, dass Deine Daten normalerweise verschlüsselt gespeichert werden. Das trifft nicht immer auf alle Daten zu, außer auf Passwörter.

Die Verschlüsselung wird durch die "Kryptographische Hashfunktion" gewährleistet, was es für Hacker unmöglich macht Dein Passwort sofort zu kennen.

Dies war die Leseprobe der Ausgabe "Digitale Vermögenswerte in Sicherheit bringen". Die gesamte Ausgabe steht Dir als Mitglied im GCExplorer zur Verfügung.

Jetzt Mitglied werden ->

Mehr Informationen ->