



Security Awareness Schulung

Carl Strömstedt



Schweizerische Post Ihr Paket ist versandfertig in der Zustellabteilung eingetroffen, geben Sie uns Ihre Lieferadresse an und bezahlen Sie die Liefergebühr, indem Sie auf den folgenden Link klicken: tinyurl.com/EHILajO



noreply@amazon.com

29.07.23

Till: noreply-3S87L@mail.assistancehelp.c... >

Your Account are on hold due to a billing issue (CaseID - 965910)

Your credit card on file has been declined.

amazon



Oh no, your Amazon Account are on hold due to a billing issue

Update Payment Information

Due to a problem with your card, we have been unable to charge your payment.

If you don't update your card information in the next 24 hours, your Amazon account are on hold permanently. To continue using your account, please [visit this link](#) to log in to your account and update your payment information.

Thank you,

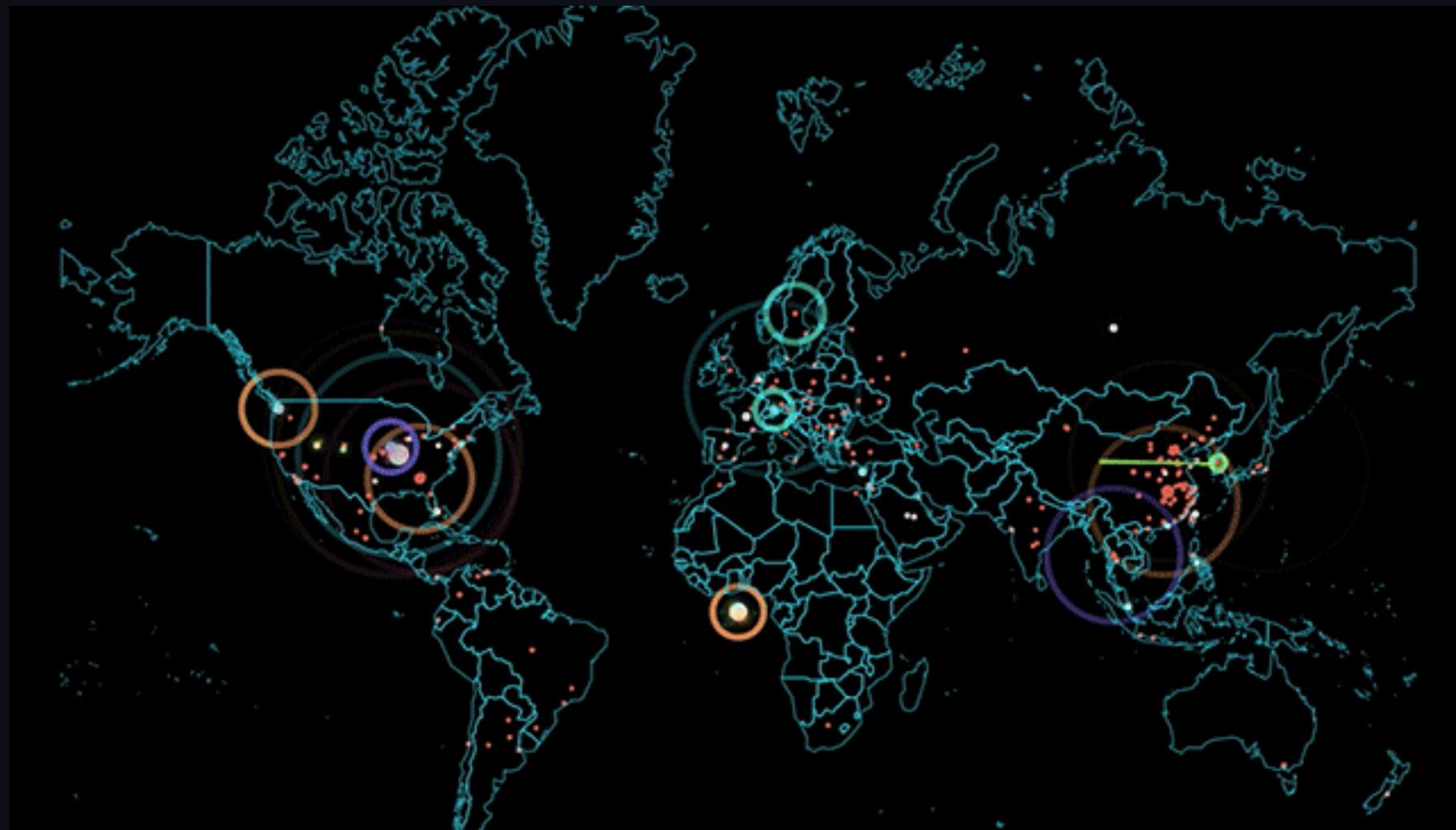
Customer Service

 Alle Mitteilungen

11. Mai 2023

Cyberangriff auf das Unternehmen NZZ: Veröffentlichung von NZZ-Daten im Darknet

Die NZZ wurde am 24. März 2023 trotz umfassender IT-Sicherheitsvorkehrungen Ziel eines Cyberangriffs durch die Ransomware-Gruppe «Play». Dank guter Vorbereitung war das Unternehmen in der Lage, den Betrieb mit nur geringen Einschränkungen aufrechtzuerhalten und den Angriff damit weitgehend einzudämmen. Die Ransomware-Gruppe «Play»

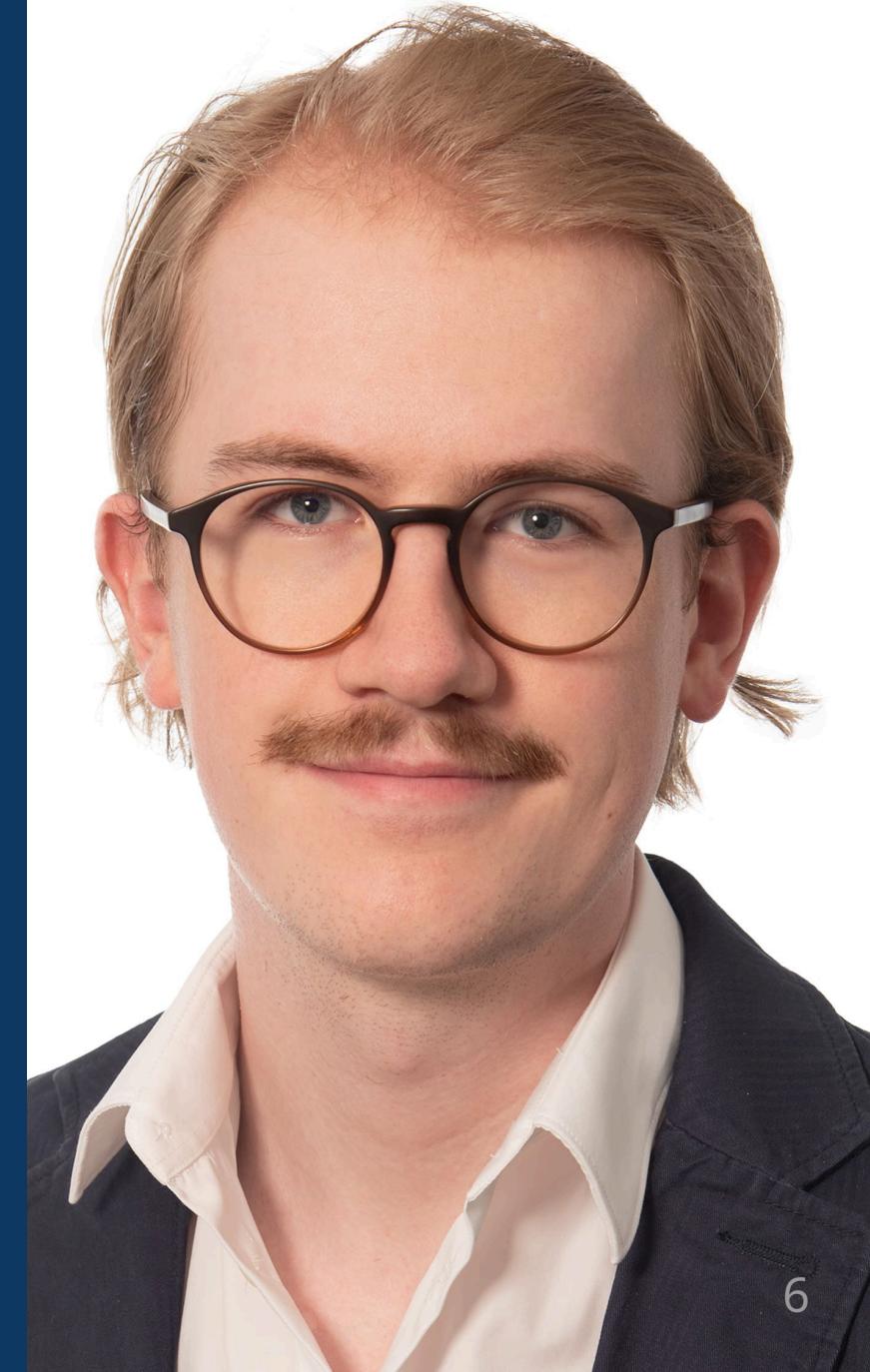


3 Blöcke

- **Informationssicherheit**
- **Malware & Phishing**
- **Passwörter & Verhaltensweisen**

Carl Strömstedt

- IT Applikationsentwickler
- Hobbies
 - Bouldern
 - Lesen
 - Reisen



Block 1

Informationssicherheit

Was bedeutet Informationssicherheit?

Informationssicherheit

- IS beinhaltet Sicherstellung der **Vertraulichkeit, Integrität und Verfügbarkeit** von Informationen.
- IS wird gewährleistet, wenn ausreichend **technische, bauliche und organisatorische** Schutzmassnahmen getroffen wurden.
- IS wird durch jeden einzelnen beeinträchtigt, gewährleistet oder verbessert.

Vertraulichkeit



Definition

Schutz vor unbefugtem Zugriff auf sensitive Informationen, um die Privatsphäre und Geheimhaltung zu wahren.



Beispiel

Nur autorisierte Mitarbeiter haben Zugang zu Finanzdaten, um sicherzustellen, dass sensible Informationen nicht öffentlich werden.



Integrität



Definition

Sicherstellung der Korrektheit und Unveränderlichkeit von Daten, um unautorisierte Manipulation oder Verfälschung zu verhindern.



Beispiel

Durch Einsatz von digitalen Signaturen wird sichergestellt, dass ein Dokument von einem bestimmten Absender stammt und unverändert ist.



Verfügbarkeit



Definition

Gewährleistung der ständigen Zugänglichkeit von Informationen und Ressourcen, um Unterbrechungen und Ausfälle zu minimieren.



Beispiel

Durch regelmäßige Wartung und redundante Serverinfrastruktur wird sichergestellt, dass eine Webseite jederzeit erreichbar ist.

Vertraulichkeit / Integrität / Verfügbarkeit - Quiz

Fallbeispiel 1

Ein Mitarbeitender findet nach einer Sitzung einen Fehler im genehmigten Protokoll. Die Bereinigung dieses Fehlers würde den Inhalt des Beschlusses verändern. Er nimmt die Änderung trotzdem vor und legt das angepasste Protokoll ohne Information an die Kollegen und Vermerk einer Änderung auf der Geschäftsablage ab.



Vertraulichkeit



Verfügbarkeit



Integrität

Fallbeispiel 1

Ein Mitarbeiter findet nach einer Sitzung einen Fehler im genehmigten Protokoll. Die Bereinigung dieses Fehlers würde den Inhalt des Beschlusses verändern. Er nimmt die Änderung trotzdem vor und legt das angepasste Protokoll ohne Information an die Kollegen und Vermerk einer Änderung auf der Geschäftsablage ab.



Vertraulichkeit



Verfügbarkeit



Integrität

Fallbeispiel 2

Ein Mitarbeiter des Verkaufs telefoniert im Zug. Er bespricht dabei lautstark Details einer Offerte, so dass den Anwesenden im Zug die betroffene Firma sowie die Schlüsselpersonen, der Umfang und die Kosten des Auftrags bekannt sind.



Vertraulichkeit



Verfügbarkeit



Integrität

Fallbeispiel 2

Ein Mitarbeiter des Verkaufs telefoniert im Zug. Er bespricht dabei lautstark Details einer Offerte, so dass den Anwesenden im Zug die betroffene Firma sowie die Schlüsselpersonen, der Umfang und die Kosten des Auftrags bekannt sind.



Vertraulichkeit



Verfügbarkeit



Integrität

Fallbeispiel 3

Es kann nicht auf wichtige Geschäftsdaten zugegriffen werden, weil der IT-Dienstleister ein kurzfristiges, unangekündigtes Wartungsfenster durchführt, um die Software zu aktualisieren.



Vertraulichkeit



Verfügbarkeit



Integrität

Fallbeispiel 3

Es kann nicht auf wichtige Geschäftsdaten zugegriffen werden, weil der IT-Dienstleister ein kurzfristiges, unangekündigtes Wartungsfenster durchführt, um die Software zu aktualisieren.



Vertraulichkeit



Verfügbarkeit



Integrität

Fallbeispiel 4

Ein Mitarbeiter klickt auf einen Link in einer Nachricht mit der Aufforderung, seinen Lotto-Gewinn einzufordern. Er bestätigt die Installation eines Zertifikats im Browser, um auf die gewünschte Seite zugreifen zu können. Sämtliche Daten, die er versendet und empfängt, werden nun von jemandem Drittem entschlüsselt, eingesehen und für einen Betrug verändert.



Vertraulichkeit



Verfügbarkeit



Integrität

Fallbeispiel 4

Ein Mitarbeiter klickt auf einen Link in einer Nachricht mit der Aufforderung, seinen Lotto-Gewinn einzufordern. Er bestätigt die Installation eines Zertifikats im Browser, um auf die gewünschte Seite zugreifen zu können. Sämtliche Daten, die er versendet und empfängt, werden nun von jemandem Drittem entschlüsselt, eingesehen und für einen Betrug verändert.



Vertraulichkeit



Verfügbarkeit



Integrität

Beispiele für wertvolle und sensitive Informationen



Zahlungsdaten



Personendaten



Gesundheitsdaten

Motivation Angreifer

Wirtschaftlich

- Eigene Bereicherung
- Elimination der Konkurrenz
- Verbessern der Marktstellung

Motivation Angreifer

Wirtschaftlich



- Eigene Bereicherung
- Elimination der Konkurrenz
- Verbessern der Marktstellung

Politisch



- Beeinflussung von Wahlen
- Imageschaden eines Konkurrenten
- Verbreitung von religiösen oder politischen Inhalten.

Motivation Angreifer

Wirtschaftlich



- Eigene Bereicherung
- Elimination der Konkurrenz
- Verbessern der Marktstellung

Politisch



- Beeinflussung von Wahlen
- Imageschaden eines Konkurrenten
- Verbreitung von religiösen oder politischen Inhalten.

Persönlich



- Bestätigung
- „For the LULZ“ (Amüsierung)



Schwachstelle

Informationen / Daten

Angreifer



Benutzt

Schwachstelle

Informationen / Daten

Angreifer



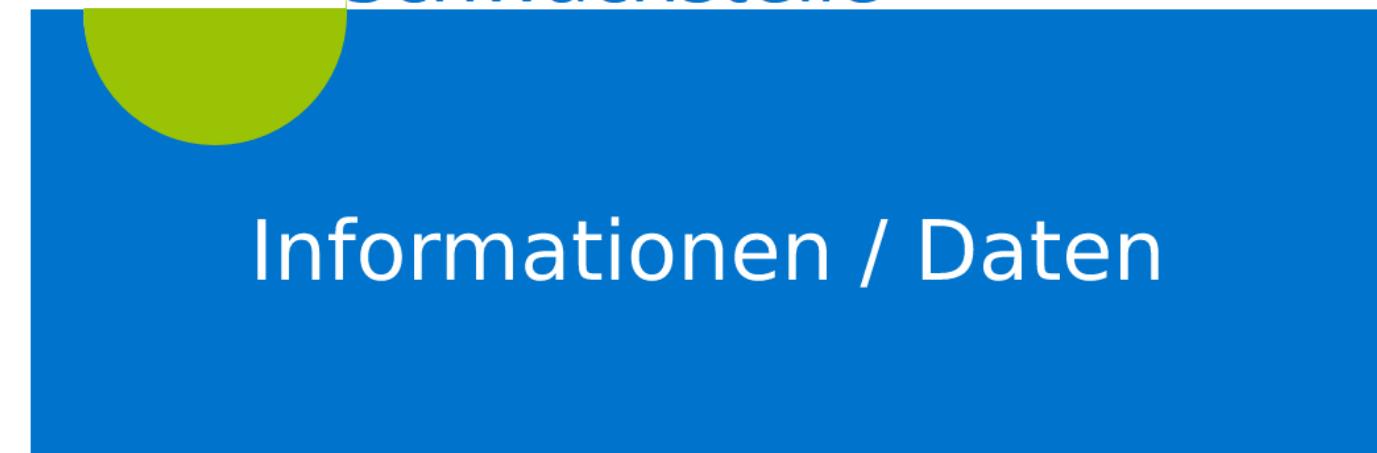
Schutzmassnahmen



Benutzt

Sichert

Schwachstelle



Angreifer

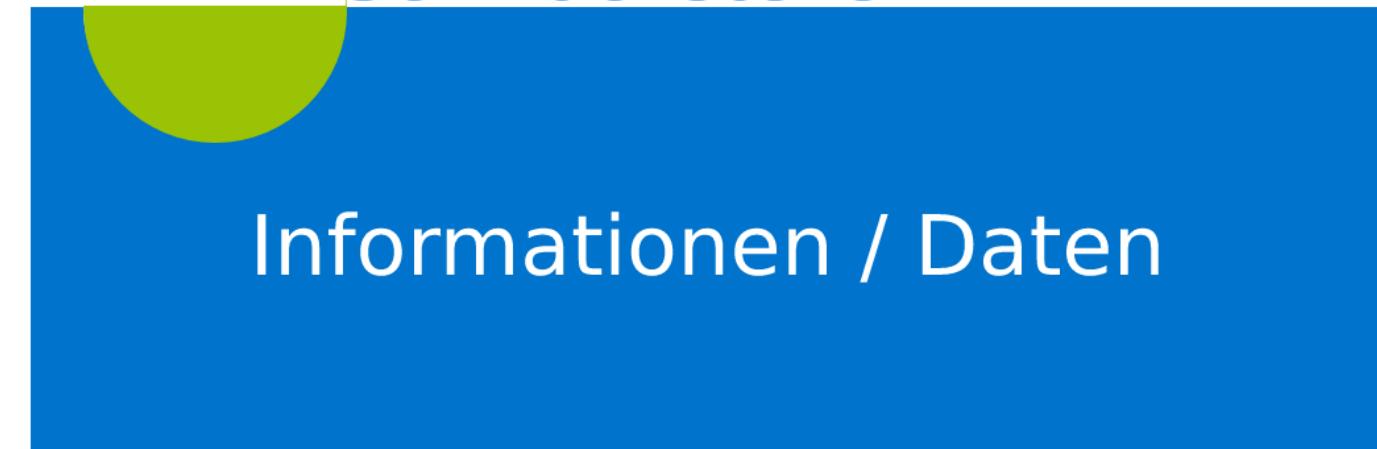


Schutzmassnahmen



Sichert

Schwachstelle



Klassifizierungen von Informationen

Anforderungen an Informationen

Vertraulichkeit 

Integrität 

Verfügbarkeit 

Klassifizierungen

Wieso?

Hilft uns Vorgaben zu Definieren

Was?

Alle Informationen und Daten

Welche Klassifizierungen?

- Vertraulich
- Intern
- Öffentlich

Vertraulich



Aufbewahrung

- Nur Berechtigte haben Zugriff

Transport

- Nur verschlüsselt und nicht telefonisch

Bearbeitung

- Kopieren nicht erlaubt & überwachter Ausdruck



Aufbewahrung

-  Alle innerhalb der Firma haben Zugriff

Transport

-  Unverschlüsselter austausch erlaubt

Bearbeitung

-  Ändern, Kopieren, Drucken bei Bedarf erlaubt

Öffentlich

Aufbewahrung

-  Alle haben Zugriff

Transport

-  Jeglicher Austausch erlaubt

Bearbeitung

- ✓ Änderungen müssen nachvollziehbar sein

Informationssicherheitsvorfälle

Beeinträchtigung der Informationssicherheit

Beeinträchtigung der Informationssicherheit



Vertraulichkeit

Wenn jemand unbefugt Einsicht in
Informationen hatte

Beeinträchtigung der Informationssicherheit



Vertraulichkeit

Wenn jemand unbefugt Einsicht in
Informationen hatte

Integrität

Wenn Informationen oder Daten beschädigt
oder verfälscht wurden

Beeinträchtigung der Informationssicherheit



Vertraulichkeit

Wenn jemand unbefugt Einsicht in Informationen hatte

Integrität

Wenn Informationen oder Daten beschädigt oder verfälscht wurden

Verfügbarkeit

Bei Datenverlust oder wenn temporär nicht darauf zugegriffen werden kann

Vorgehen bei einem Sicherheitsvorfall



Verdacht

- Wenn du etwas Verdächtiges bemerkst, zögere nicht und melde dich bei uns.



Melden

- Am besten meldest du dich telefonisch oder erstellst ein Support-Ticket.



Weiterleiten

- Verdächtige Phishing-E-Mails bitte an support@open-circle.ch weiterleiten.

Was macht Open Circle dagegen?



DNS-Filtering



Spam-Filtering



Regelmässige Updates von Server & Clients



2-Faktor-Authentifizierung



Awareness-Schulungen

Erster Block - Fazit

Erster Block - Fazit

3 Schutzziele

- Vertraulichkeit
- Integrität
- Verfügbarkeit

Risiko

Schwachstellen durch
Schutzmassnahmen sichern

3 Klassifizierungen

- Vertraulich
- Intern
- Öffentlich

Sicherheitsvorfall

Unsicher? Misstrauisch?
→ Melden

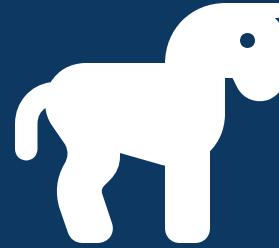
Erster Block - Quiz

Block 2

Malware & Phishing



Viren



Trojaner



Spyware



Ransomware



Viren

Schadprogramme, die sich durch Einschleusung in andere Systeme verbreiten



Verbreitung

Durch infizierte Dateien, E-Mail-Anhänge oder infizierte Webseiten.



Trojaner

Tarnen sich als legitime Software, um unbemerkt in Systeme einzudringen.

Öffnet Hintertüren, stiehlt Daten oder ermöglicht Fernsteuerung.



Verbreitung

Durch gefälschte E-Mail-Anhänge, infizierte Downloads oder Drive-by-Downloads.



Spyware

Sammelt heimlich Informationen über Nutzer*innen und ihre Aktivitäten.



Verbreitung

Durch Software-Bündelung, infizierte Links oder Drive-by-Downloads.



Ransomware

Sperrt oder verschlüsselt Daten, fordert Lösegeld zur Wiederherstellung.



Verbreitung

Durch infizierte E-Mail-Anhänge, Exploit-Kits oder schadhafte Downloads.



Beispiel: WannaCry-Virus

- Ausbruch im Mai 2017
- Ransomware, die weltweit Windows-Systeme befiel.



Ziel und Auswirkungen

- Ausnutzung der Windows-Schwachstelle "EternalBlue"
- Betraf Organisationen wie die NHS (UK) und FedEx



Verbreitung und Komplexität

- Schnell weltweit verbreitet, über 230.000 Systeme in 150 Ländern
- Verschlüsselte Daten und forderte Bitcoin-Lösegeld



Lehren

- Bedeutung von regelmässigen Updates und Backups
- Zeigt die Verwundbarkeit von Systemen ohne Sicherheits-Patches

 Wana Decrypt0r 2.0

English



What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Payment will be raised on
5/15/2017 16:32:52

Time Left
02:23:59:49

Your files will be lost on
5/19/2017 16:32:52

Time Left
06:23:59:49

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am (UTC+00:00) Monday-Friday

Send \$300 worth of bitcoin to this address:

 **12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw**

Contact Us

Check Payment **Decrypt**

Angriffskomponenten

Was verwenden die Angreifer für ihre Attacken?

Technik 

Soziale Ebene 

Technik

- Drive-by-Download 
- E-Mail-Anhänge 
- Software-Bündelung 



Drive-by-Download

Automatischer Download von Malware beim Besuch einer infizierten Webseite.



Mechanismus

Ausnutzung von Sicherheitslücken im Browser oder Plugins, um Schadcode einzuschleusen.

Authorized Drive-by Downloads Explained



Hacker creates a corrupt link, email, website, or ad.

You willingly click on or download the infected link or attachment.

Malware installs, and the hacker gains access to your system.

Unauthorized Drive-by Downloads Explained



1
Hacker
infects a
legitimate
website.

2
You visit the
infected page
and/or click on the
corrupt element.

3
Malware
downloads
onto your
device.



E-Mail-Anhänge

Anhänge die beim öffnen Schwachstellen in Software (wie Dokumentenlesern) ausnützen, um Malware zu installieren.



Mechanismus

Ausnutzung von Software-Schwachstellen, Ausführen von Makros



Software-Bündelung

Malware wird zusammen mit legitimer Software gebündelt und bei der Installation mit installiert.



Mechanismus

Nutzer:innen bemerken die Malware oft nicht, da sie vertrauenswürdige Software als Tarnung verwendet.



Rootkits

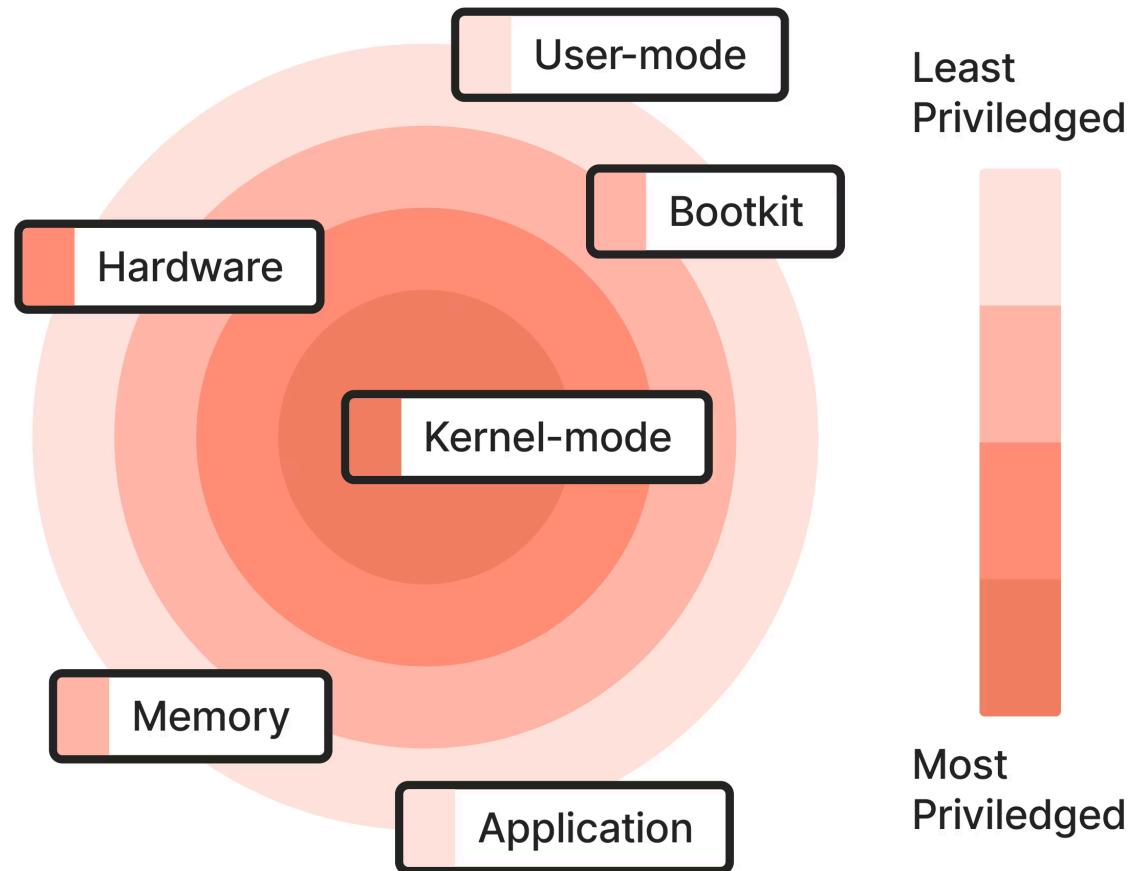
Rootkits sind bösartige Software, die tief in ein Computersystem eindringt und Zugriff auf verschiedenen Ebenen erhält.



Mechanismus

Durch Zugriff auf Systemebene können Rootkits Administrationsbefugnisse erlangen und Systeme kompromittieren.

Types of Rootkits





Schutz vor Malware



Softwareaktualisierungen

Halte dein Betriebssystem und alle Programme auf dem neuesten Stand, um bekannte Sicherheitslücken zu schließen.



Vorsicht bei E-Mails

Öffne keine E-Mail-Anhänge oder klicke nicht auf Links von unbekannten oder verdächtigen Absendern.



Verhaltensbewusstsein

Sei vorsichtig beim Herunterladen von Dateien aus dem Internet und vermeide fragwürdige Webseiten.

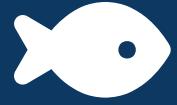
Soziale Ebene

Social Engineering

Manipulation von Menschen, durch ausnutzung von Vertrauen, Neugier oder Druck, um vertrauliche Informationen preiszugeben oder unerlaubte Handlungen auszuführen.

Methoden

- Phishing
- Vishing (Telefon)



Phishing

Täuschung von Nutzer:innen, um vertrauliche Informationen wie Passwörter oder Finanzdaten zu stehlen.



Methoden

Gefälschte E-Mails, Webseiten oder soziale Medien, die echt aussehen, um Vertrauen zu erwecken.

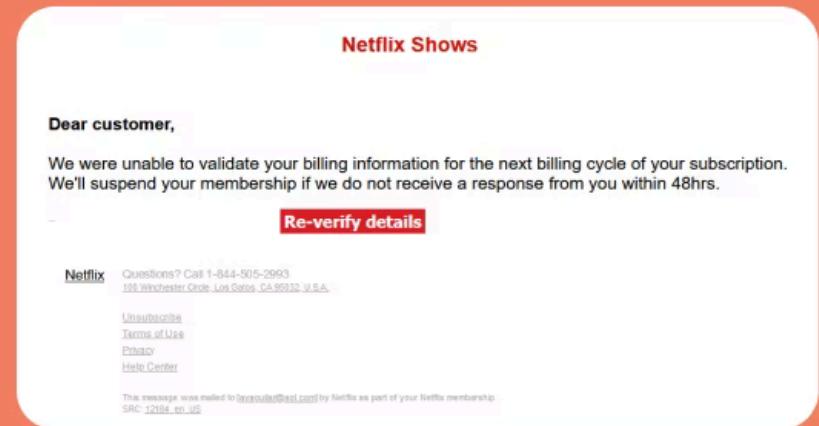
Account Information Alert

ə'kaʊnt ɪnfər'meɪʃən ə'lɜrts / noun

01. An email or text sent to an individual by a service provider they are signed up with.

Your Netflix membership has been ended, because we're having some trouble with your current account information.

02. A scam that involves notifying a recipient of the need to update their account information, usually payment details.



Account Suspension

ə'kaʊnt sə'spenʃən / verb

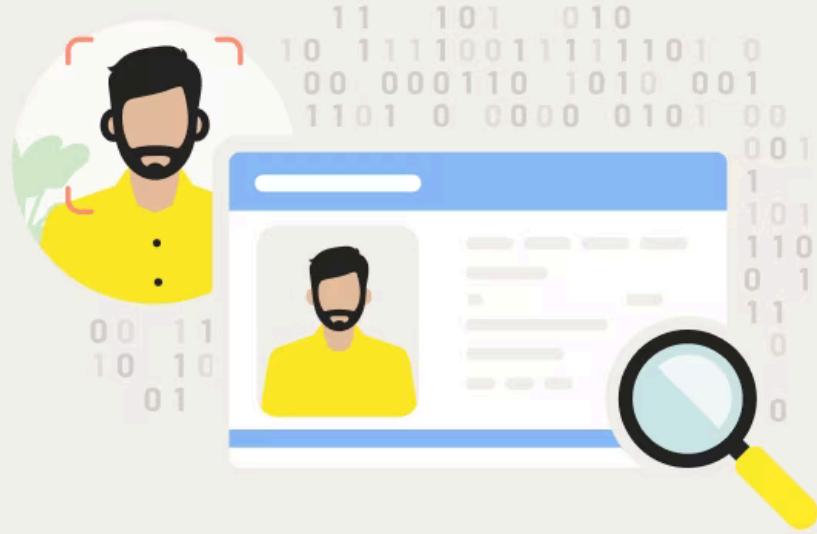
01. A message received asking the recipient to restore their suspended account.

Your Apple Pay has been suspended, please update your details by visiting: </url/>

02. A fake message addressed to an individual asking them to complete account recovery within a specific time period otherwise it will result in permanent suspension.

We temporarily place your Paypal suspended, To restore follow instruction below. </url/> Please complete the recovery within 2 days otherwise Paypal account permanently suspended. We are sorry for any inconvenience has caused. Thank you for your attention.





Account Verification

vərəfə'keɪʃən / noun

01. A fraudulent email sent by scammers that looks like a message from a contact of a well-known entity with the goal to extract account login credentials.

New login detected from: [Country name] Windows 10 Follow link below to unlock your account: </url/> verify your account within 24 hours or your PayPal account will be terminated permanently.

Regards, PayPal



account-report@cs-amazon.com... torsdag

Verify your info : account temporiraly disable - Action required. Help- CS #411.125951.2451



Your Amazon account has been put on hold, therefore your last order, and subscriptions will be temporary on hold.

We took this action, because the billing information you provided did not match with the information of the card issuer data. which is **Violating our terms of service.**

Please update your information as soon as possible so you can continue using your Amazon account.

[Update Information](#)

In order to maintain the safety of your account, your account will be locked until you fulfill the required forms.

You might want to do this sooner, any locked account will be deleted in order to protect the data from being leaked.

We hope to see you again soon,
Sincerely,
Amazon Team Support

Login Attempts

loginə'tempts / verb



01. A message notifying the receiver that an unknown user has tried to access their account.

CommBank Alert: A login was made from an Unknown Location: Melbourne, VIC. Not you? Please review now visit: </url|>

02. An attempt to trick somebody into thinking their account has been hacked, to convince them to share personal information.

RBC Alert : Your online account is temporarily locked due to an unusual sign in attempt. Please login and confirm your information. </url|>



New login from an unknown device detected.

We've just noticed an unusual unknown device logged in with your account details. Since we don't recognize the device, we've placed some limits on your account.

Please [Click Here](#) and complete the required task's to remove the limits

Malware Threats

mælwærəts / noun

01. A technique used by cybercriminals to trick people into thinking their device has been infected with malware.

DANGER: A THREAT has INFECTED your LAPTOP! ACT NOW to PROTECT your CONFIDENTIAL FILES at </url/>





Scare Tactic

skær'tæktrɪks / verb

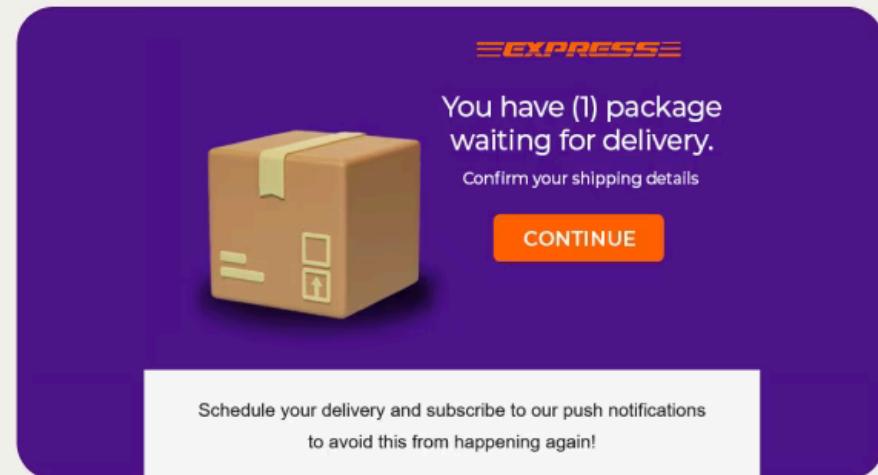
01. A common scam tactic that often uses fearmongering and urgency to steal personal or financial information.

Your payment is overdue. Please avoid your fine charge please see <url>

Shipping Scams

ſípiŋ skæmz / noun

01. A message received by a customer detailing delivery information and requesting delivery or payment preferences.
Hi Your FEDEX parcel with tracking <number> is waiting for you to set delivery preferences: <url>





Mi. 28.09.2016 11:18

Andreas Nickel <duffybee@t-online.de>
erika.meier Achtung – Erste Mahnung (Bäckerei-Lebensmittel)

An erika.meier@ebas.ch



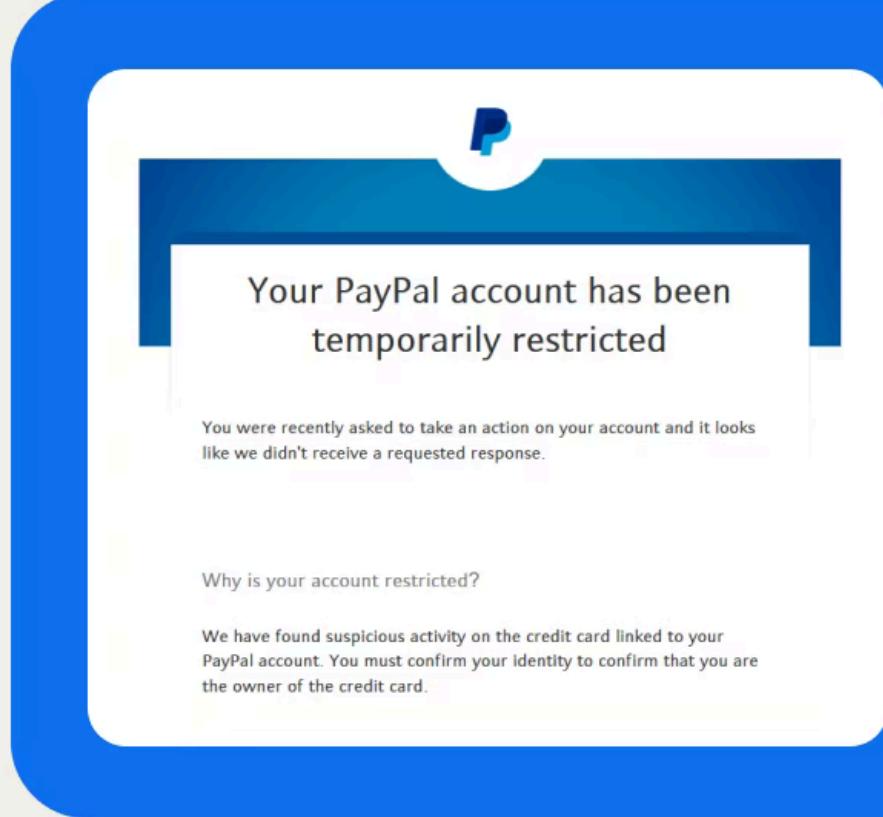
Sehr geehrte(r) Frau (Herr) erika.meier,

Die Pendenz von 2,657.00 CFr. mit der Bestellnummer 1SW-0789054 ist bis jetzt nicht beglichen worden. Gerne lege ich Ihnen eine zusätzliche Kopie Ihrer Zahlungsinformationen bei.

Ferner noch eine freundliche Erinnerung: Falls die Zahlung nicht innert der nächsten 28 Tage auf unserem Konto eintrifft, behalten wir uns vor, erheben wir Anspruch, Ihrem Konto weitere Mahnkosten zuzurechnen. Diese sind in den allgemeinen Geschäftsbedingungen ausführlich aufgeführt.

Freundlichst grüßt Sie,
Andreas Nickel
Fluora Leuchten AG

Schweizerische Post Ihr Paket ist versandfertig in der Zustellabteilung eingetroffen, geben Sie uns Ihre Lieferadresse an und bezahlen Sie die Liefergebühr, indem Sie auf den folgenden Link klicken: [tinyurl.com/
EHILajO](http://tinyurl.com/EHILajO)



Suspicious Activity

sə'spiʃəs æk'tivəti / verb

01. A phrase that refers to a type of email scam targeting online customers.
Amazon: your account has been locked due to suspicious activity: <url>. Click the link below to unlock your account.

02. A phrase referring to an email that appears to be sent directly from an online store, notifying the recipient that their personal account has been locked.
Coinbase: your account has been locked due to suspicious activity. Click the link below to unlock your account: <url>



Datei

Nachricht

Was möchten Sie tun?



Sa. 02.07.2016 20:18

PayPal <noreply@paypal.ch>

Verdächtige Aktivität

An max

Wenn Probleme mit der Darstellungsweise dieser Nachricht bestehen, klicken Sie hier, um sie im Webbrowser anzuzeigen.



Transaktionscode: 148163129749735

Guten Tag Max Muster,

Unser Sicherheitssystem hat festgestellt, dass unberechtigte Personen versucht haben sich Zugang zu Ihrem PayPal Konto zu verschaffen.

Ihr PayPal Konto wurde daraufhin umgehend gesperrt und wird nach erfolgreicher Überprüfung Ihrer persönlichen Daten wieder für Sie freigeschaltet.

Anschließend können Sie Ihr PayPal Konto wie gewohnt weiter benutzen.

Um die Sicherheit Ihres Konto weiterhin gewährleisten zu können, bitten wir Sie um eine kurze Überprüfung Ihrer Daten.

Familie: Kuhn

IP: 193.74.160.30

Land: Bahamas

<https://fan.lu/bqstv>

Klicken oder tippen Sie, um dem Link zu folgen.

Zur Paypal-Seite

Die Ziel-Adresse der Schaltfläche «Zur Paypal-Seite» zeigt auf eine Internetadresse (fan.lu), welche nicht zu PayPal gehört.



Aktuell Cyberbedrohungen Informationen für NCS Strategie Dokumentation Über das BACS

BACS Startseite > Aktuell > Aktuelle Vorfälle

[BACS Startseite](#)

Aktuell

Im Fokus

Aktuelle Vorfälle

Aktuelle Zahlen

Newsletter

Aktuelle Vorfälle



[Phishing im Namen der AHV](#)

Derzeit erhält das BACS Meldungen bezüglich Phishing-Nachrichten im Namen der AHV. Den Empfängern wird dabei eine angebliche Rückerstattung in Aussicht gestellt. Beim Anklicken des Links muss man die Kreditkartendaten angeben. Melden Sie diese Mails dem BACS (<https://www.report.ncsc.admin.ch/de/>) und klicken Sie nicht auf den Link.

04.11.2024 10:00

[Vorsicht Schadsoftware!](#)

Derzeit erreichen uns Meldungen über E-Mails, die vorgeben, von der Bundesverwaltung zu stammen und in denen behauptet wird, dass ab Juli 2024 die Installation des "AGOV Access" für den Zugang zu öffentlichen Online-Diensten verpflichtend sei. Beim Anklicken wird man aufgefordert, eine Software zu installieren. Vorsicht: Dabei handelt es sich um Schadsoftware. Löschen Sie die E-Mail.

28.06.2024 09:10



Vishing



Was ist Vishing?

- Vishing steht für "Voice Phishing"
- Eine Betrugsmethode, bei der Betrüger sich am Telefon als legitime Organisationen ausgeben, um vertrauliche Informationen zu erlangen.



Schutz

- Sei misstrauisch gegenüber unerwarteten Anrufern
- Verifiziere die Identität des Anrufers
- Gib niemals vertrauliche Informationen am Telefon preis



Dumpster Diving

Suchen nach sensiblen Informationen in physischem Müll, um Zugriff auf vertrauliche Daten zu erhalten.



Ziel

Papierdokumente, veraltete Hardware, ungeschredderte Informationen.



Phishing-Erkennung



Grammatik und Anrede

Achte auf schlechte Grammatik und allgemeine Anreden wie "Sehr geehrte Damen und Herren".



Unrealistische Angebote

Wenn etwas zu gut klingt, um wahr zu sein, ist es wahrscheinlich nicht echt.



Sensible Datenanfragen

Gib niemals sensible Informationen aufgrund von E-Mail-Anfragen weiter. Die meisten Institutionen würden solche Informationen niemals per E-Mail anfordern.



Unbekannte Absender

Lösche unaufgeforderte E-Mails von unbekannten Absendern oder Diensten, die du nicht nutzt. Öffne sie nicht und klicke nicht auf Links oder Anhänge.



Zeitdruck

Sei misstrauisch bei E-Mails, die dringendes Handeln erfordern. Betrüger erzeugen oft künstlichen Druck, um dich zum überstürzten Handeln zu bewegen.



Falsche E-Mail-Adressen und Domänennamen

Prüfe verdächtige E-Mails auf korrekte Absenderadressen und Domänennamen. Impulsives Handeln könnte dazu führen, subtile Details zu übersehen.

Von: UBS Schweiz [<mailto:tlensch@fathomrealty.com>]

Gesendet: Montag, 16. April 2018 15:44

An: 'Max Muster' <max.muster@musterfirma.com>

Betreff: Ihr E-Banking wurde gesperrt!



Sehr geehrter Kunde,

kürzlich zeigten unsere Aufzeichnungen, dass Ihr UBS-Konto durch Dritte einen unbefugten Zutritt hatte.

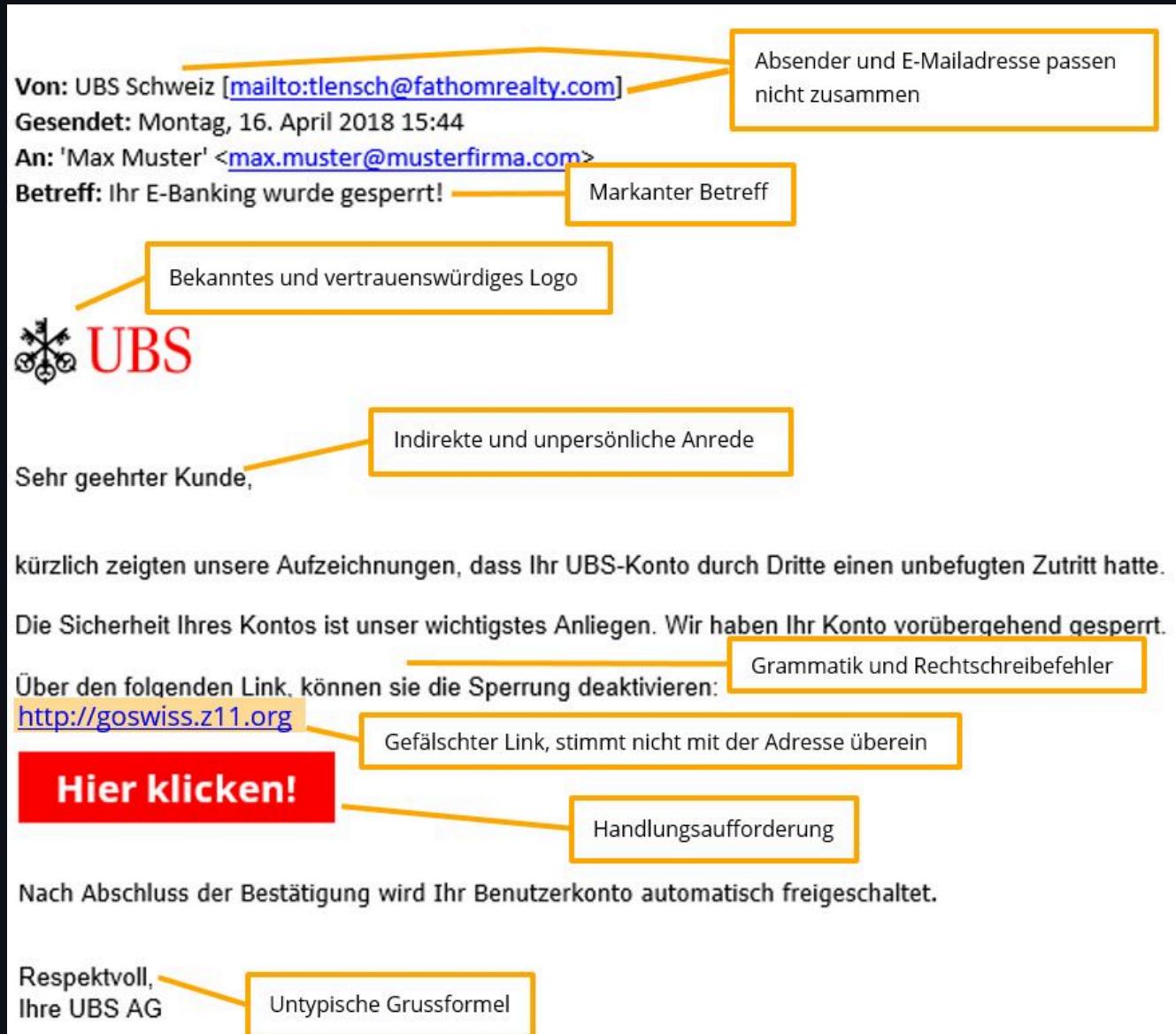
Die Sicherheit Ihres Kontos ist unser wichtigstes Anliegen. Wir haben Ihr Konto vorübergehend gesperrt.

Über den folgenden Link, können Sie die Sperrung deaktivieren:

Hier klicken!

Nach Abschluss der Bestätigung wird Ihr Benutzerkonto automatisch freigeschaltet.

Respektvoll,
Ihre UBS AG



Warum E-Mail-Signatur?



Authentifizierung

- E-Mail-Signaturen dienen der Identitätsbestätigung des Absenders.



Vertrauenswürdigkeit

- Hilft bei der Erkennung von Phishing und gefälschten E-Mails.



Integrität

- Gewährleistet, dass die Nachricht unverändert beim Empfänger ankommt.



SSL- & TLS-Zertifikate



Funktion

- SSL-Zertifikate dienen der Sicherheit und Verschlüsselung von Datenübertragungen im Internet.



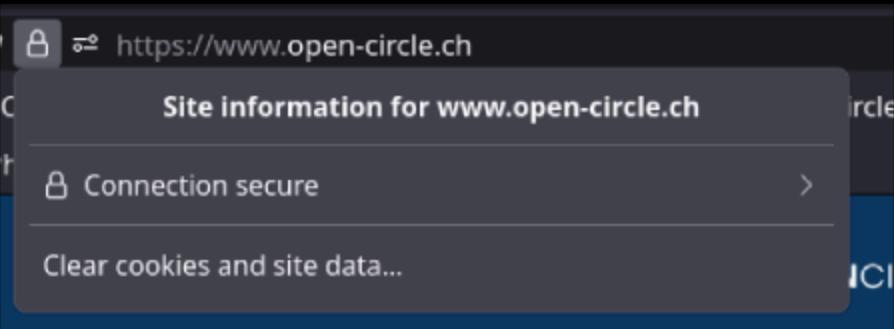
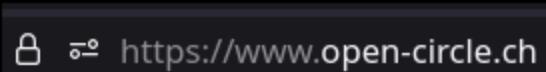
Vertrauen und Validierung

- Browser vertrauen Websites mit gültigen SSL-Zertifikaten.
- Zertifikate werden von Zertifizierungsstellen (CAs) ausgestellt und validiert.



Visuelle Hinweise

- Browser zeigen visuelle Hinweise für sichere Verbindungen, wie ein geschlossenes Vorhängeschloss oder "https" im URL.



Page Info — https://www.open-circle.ch/

General Media Permissions Security

Website Identity

Website: www.open-circle.ch
Owner: This website does not supply ownership information.
Verified by: Let's Encrypt [View Certificate](#)

Privacy & History

Have I visited this website prior to today? Yes, 83 times

Is this website storing information on my computer? Yes, cookies and 23.3 MB of site data [Clear Cookies and Site Data](#)

Have I saved any passwords for this website? No [View Saved Passwords](#)

Technical Details

Connection Encrypted (TLS_AES_256_GCM_SHA384, 256 bit keys, TLS 1.3)
The page you are viewing was encrypted before being transmitted over the Internet.

Certificate

www.open-circle.ch R3 ISRG Root X1

Subject Name

Common Name www.open-circle.ch

Issuer Name

Country US
Organization Let's Encrypt
Common Name R3

Validity

Not Before Thu, 31 Aug 2023 20:04:24 GMT
Not After Wed, 29 Nov 2023 20:04:23 GMT

Subject Alt Names

DNS Name www.open-circle.ch

Wie funktioniert Verschlüsselung?

Verschlüsselung

- Schutz von vertraulichen Informationen vor unbefugtem Zugriff.
- Nachrichten werden in eine nicht lesbare Form umgewandelt.

Schlüssel

- Ein Schlüssel wird benötigt, um die verschlüsselte Nachricht zu entschlüsseln.
- Öffentliche Schlüssel für Verschlüsselung, private Schlüssel für Entschlüsselung.

Verfahren

- Symmetrische Verschlüsselung: Derselbe Schlüssel für Verschlüsselung und Entschlüsselung.

- Asymmetrische Verschlüsselung: Zwei Schlüssel, öffentlich und privat

Symmetrische und Asymmetrische Verschlüsselung im Vergleich

Symmetrische Verschlüsselung



Asymmetrische Verschlüsselung





Verschlüsselung - Anwendungsbereiche



SSL / TLS



Verschlüsselte E-Mails



SSL / TLS

Zweiter Block - Fazit

Zweiter Block - Fazit

Malware

- Viren
- Trojaner
- Spyware
- Ransomware

Technik

- Drive-by-Download
- Drive-by-Installer
- E-Mail-Anhänge
- Software-Bündelung

Soziale Ebene

- Phishing
- Vishing (Telefon)

Social Engineering

Manipulation von Menschen durch ausnutzung von Emotionen

Zweiter Block - Quiz

Block 3

Passwörter & Verhaltensweisen

Authentisierung

Benutzer*in gibt Benutzernamen und Passwort ein

Behauptung einer Identität

Authentifizierung

Server prüft bestehende Nutzer*innen auf Benutzername und Passwort

Überprüfung der Identität

Autorisierung

Welche Aktionen oder Ressourcen ein authentifizierter Benutzer ausführen darf



Formen



Wissen (Passwörter)

- Benutzername und geheimes Passwort
- Anfällig für Phishing und soziale Ingenieurstechniken



Besitz (Physische Keys)

- Hardware-Token, Smartcards, USB-Schlüssel
- Erhöhte Sicherheit, benötigt physischen Zugriff



Biometrie

- Fingerabdruck, Gesichtserkennung, Iris-Scan



Brute Forcing



Was ist Brute Forcing?

- Methode, bei der alle möglichen Kombinationen ausprobiert werden
- Ziel: Passwort oder geheime Informationen erraten



Beispiel

- Passwort: "Secure123-"
- Theoretische zeit zum Knacken: Seconds



Wörterlisten kürzen die Zeit drastisch

Secret123-

Very Weak

10 characters containing:

Lower case

Upper case

Numbers

Symbols

Time to crack your password:
4.39 seconds

Review: Oh dear, using that password is like leaving your front door wide open. Your password is very weak because it contains a common password and a sequence of characters.

Sc|ret123-

Very Strong

9 characters containing:

Lower case

Upper case

Numbers

Symbols

Time to crack your password:

7 years

Review: Fantastic, using that password makes you as secure as Fort Knox.

/// Dominoeffekt bei Mehrfachverwendung



Was verursacht den Dominoeffekt?

- Verwendung desselben Passworts für verschiedene Konten



Gefahren

- Angreifer nützen diese Schwachstelle aus
- Ein geknacktes Passwort ermöglicht Zugriff auf andere Konten

';--have i been pwned?

Check if your email address is in a data breach

pwned?

Oh no — pwned!

Pwned in 16 data breaches and found no pastes ([subscribe to search sensitive breaches](#))

[!\[\]\(1502a00c919786c8095639fea3937464_img.jpg\)](#) [!\[\]\(380f8b1fd4ae11cbc71b6ec7ef885eba_img.jpg\)](#) [!\[\]\(93d8af702ff50f41040b8174d8e17e13_img.jpg\)](#) [!\[\]\(7da30a0153a5fdf8155b677d2af0df37_img.jpg\)](#) [Donate](#)

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the [1Password password manager](#) helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.



Adobe: In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the *passwords* adding further to the risk that hundreds of millions of Adobe customers already faced.

Compromised data: Email addresses, Password hints, Passwords, Usernames

Section #1					
		File Manager			
		NEW combo semi private > Dumps			
		Name	Größe	Typ	Uploaddatum
		www.hundesalon-lili.at {56.463} [NOHASH].txt	1.8 MB	Text Document	2018-12-15 07:16
		www.huntclublisting.com {13.857} [NOHASH].txt	456 KB	Text Document	2018-12-15 07:16
		www.hypnoseries.tv {102.497} [NOHASH].txt	2.9 MB	Text Document	2018-12-15 07:16
		www.ias100.in {257.343} [NOHASH].txt	8.4 MB	Text Document	2018-12-15 07:16
		www.icontrolpollution.com {44.94} [NOHASH].txt	1.4 MB	Text Document	2018-12-15 07:16
		www.immersionprograms.com {11.12} [NOHASH].txt	379 KB	Text Document	2018-12-15 07:16
		www.ineedtutor.ru {10.103} [NOHASH].txt	245 KB	Text Document	2018-12-15 07:16
		www.innovationreview.eu {24.269} [NOHASH].txt	720 KB	Text Document	2018-12-15 07:16
		www.integrame.ro {31.232} [NOHASH].txt	1002 KB	Text Document	2018-12-15 07:16
		www.interlinepublishing.com {8.126} [NOHASH].txt	259 KB	Text Document	2018-12-15 07:16
		www.investingwithinsight.com {9.560} [NOHASH].txt	293 KB	Text Document	2018-12-15 07:16
		www.iregisteredonline.com {9.166} [NOHASH].txt	292 KB	Text Document	2018-12-15 07:16
		www.irg-listings.com {9.778} [NOHASH].txt	320 KB	Text Document	2018-12-15 07:16
		www.islandpages.com {16.466} [NOHASH].txt	500 KB	Text Document	2018-12-15 07:16
		www.italiansonline.net {170.663} [NOHASH].txt	5.2 MB	Text Document	2018-12-15 07:16
		www.itotal.ru {508.490} [NOHASH].txt	13.0 MB	Text Document	2018-12-15 07:16
		www.japanese-edu.org.hk {112.970} [NOHASH].txt	3.4 MB	Text Document	2018-12-15 07:16
		www.kazachok.com {42.738} [NOHASH].txt	1.4 MB	Text Document	2018-12-15 07:16
		www.kepzeslista.hu {11.543} [NOHASH].txt	343 KB	Text Document	2018-12-15 07:16
		www.kesar.club {10.135} [NOHASH].txt	325 KB	Text Document	2018-12-15 07:16
		www.kffl.com {127.097} [NOHASH].txt	4.2 MB	Text Document	2018-12-15 07:16
		www.kimjusa.com {26.915} [NOHASH].txt	741 KB	Text Document	2018-12-15 07:16
		www.klup.nl {227.314} [NOHASH].txt	7.1 MB	Text Document	2018-12-15 07:16
		www.knowyourcollege-gov.in {72.178} [NOHASH].txt	2.3 MB	Text Document	2018-12-15 07:16
		www.korea-fever.net {37.123} [NOHASH].txt	1.2 MB	Text Document	2018-12-15 07:16
		www.kutatokejszakaja.hu {64.211} [NOHASH].txt	2.0 MB	Text Document	2018-12-15 07:16
		www.lavera.co.jp {101.794} [NOHASH].txt	3.3 MB	Text Document	2018-12-15 07:16
		www.le-sentier-paris.com {36.177} [NOHASH].txt	1.1 MB	Text Document	2018-12-15 07:16
		www.leadersinfitness.com {34.804} [NOHASH].txt	1.1 MB	Text Document	2018-12-15 07:16
		www.lexisnexis-conferences.com {24.164} [NOHASH].txt	665 KB	Text Document	2018-12-15 07:16
		www.lezec.cz {9.679} [NOHASH].txt	301 KB	Text Document	2018-12-15 07:16
		www.limmobiliareagrado.it {12.288} [NOHASH].txt	365 KB	Text Document	2018-12-15 07:16
		www.listfire.com {220.769} [NOHASH].txt	6.5 MB	Text Document	2018-12-15 07:16
		www.livingnature.info {82.314} [NOHASH].txt	2.7 MB	Text Document	2018-12-15 07:16



Passwortempfehlungen

12 Mindestlänge von 12 Zeichen

Klein- und Gross-Buchstaben, Zahlen und Sonderzeichen

↔ Benutze Eselsbrücken mit Anfangsbuchstaben anstatt Wörter

• Verwende für jedes Konto ein einzigartiges Passwort

☰ Nutze Passwort-Manager zur Verwaltung

🔑 Multi-Faktor-Authentifizierung (MFA) verwenden

Passwort-Manager

Warum Passwort-Manager?

- Speichert und verwaltet sichere Passwörter
- Erzeugt zufällige, komplexe Passwörter

Vorteile

- Kein Auswendiglernen nötig
- Schützt vor Mehrfachverwendung von Passwörtern

Funktionsweise

- Master-Passwort für den Zugriff
- Sichere Speicherung verschlüsselter Passwortdaten

Verhaltensweisen

Verhalten in öffentlichen Netzwerken 

Clean-Desk-Policy 



Verhalten in öffentlichen Netzwerken



Öffentliche Netzwerke

- Gefahr von MitM-Angriffen und Datenspionage
- Vermeide Online-Banking und sensitive Aktivitäten



Verhaltenstipps

- Deaktiviere Dateifreigabe und Netzwerkfreigaben
- Verwende sichere Websites (HTTPS)
- Nutze VPN für verschlüsselte Verbindung



Virtuelles Privates Netzwerk (VPN)

- Verschlüsselt Internetverkehr über sicheren Tunnel



Clean Desk Policy



Warum eine Clean Desk Policy?

Die Clean Desk Policy hilft bei der Wahrung der VIV-Prinzipien:

- Vertraulichkeit
- Integrität
- Verfügbarkeit



Sicherheitsrisiken

Ein nicht aufgeräumter Arbeitsplatz kann Sicherheitsrisiken bergen:

- Benutzung eines eingeloggten Nutzerkontos
- Einblick in vertrauliche Unterlagen



Umsetzung

Die Policy beinhaltet:

- Regelmäßiges Aufräumen des Arbeitsplatzes
- Ausloggen bei Verlassen
- Keine Hinweise auf vertrauliche Daten



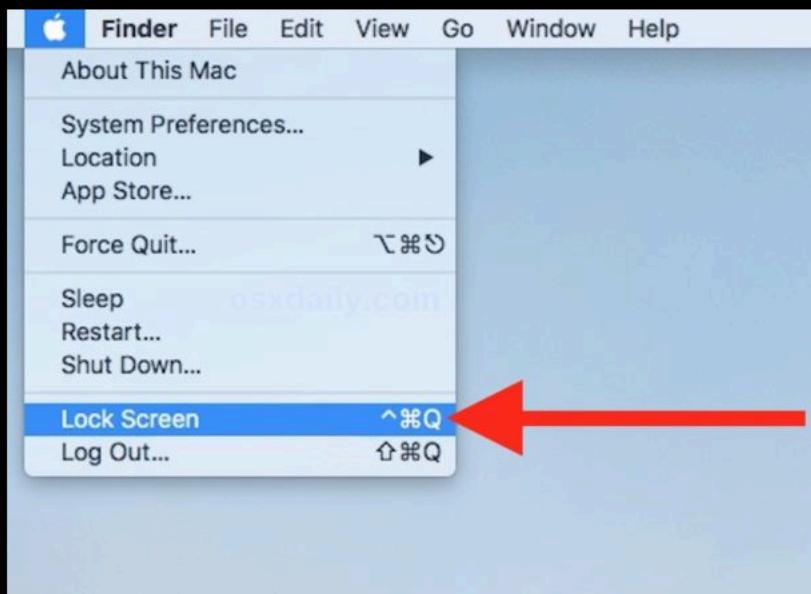
Schutz vor Spionage

Verhindert Spionage durch:

- Eigene Angestellte
- Anheuerung von Drittpersonen
- Identitätsmissbrauch

Locking your screen

Mac



Windows



Linux

Ctrl+Alt+L or Super+L

Or short press the power button

Dritter Block - Fazit

Dritter Block - Fazit

Passwortempfehlungen

- Verwende für jedes Konto ein einzigartiges Passwort
- Nutze Passwort-Manager zur Verwaltung
- Multi-Faktor-Authentifizierung (MFA) verwenden

Clean-Desk-Policy

Die Clean Desk Policy hilft bei der Wahrung der VIV-Prinzipien

Bildschirm sperren!

Dritter Block - Quiz

Links

- E-Mail Adresse prüfen

<https://haveibeenpwned.com>

- Passwort prüfen

<https://haveibeenpwned.com/passwords>

- Nationales Zentrum für Cybersicherheit:

<https://www.ncsc.admin.ch/ncsc/de/home.html>

- Information is beautiful

<https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

- Phishing quiz

<https://phishingquiz.withgoogle.com/>



Open Circle AG
Freilagerstrasse 32
8047 Zürich



carl.stroemstedt@open-circle.ch



044 552 13 86

