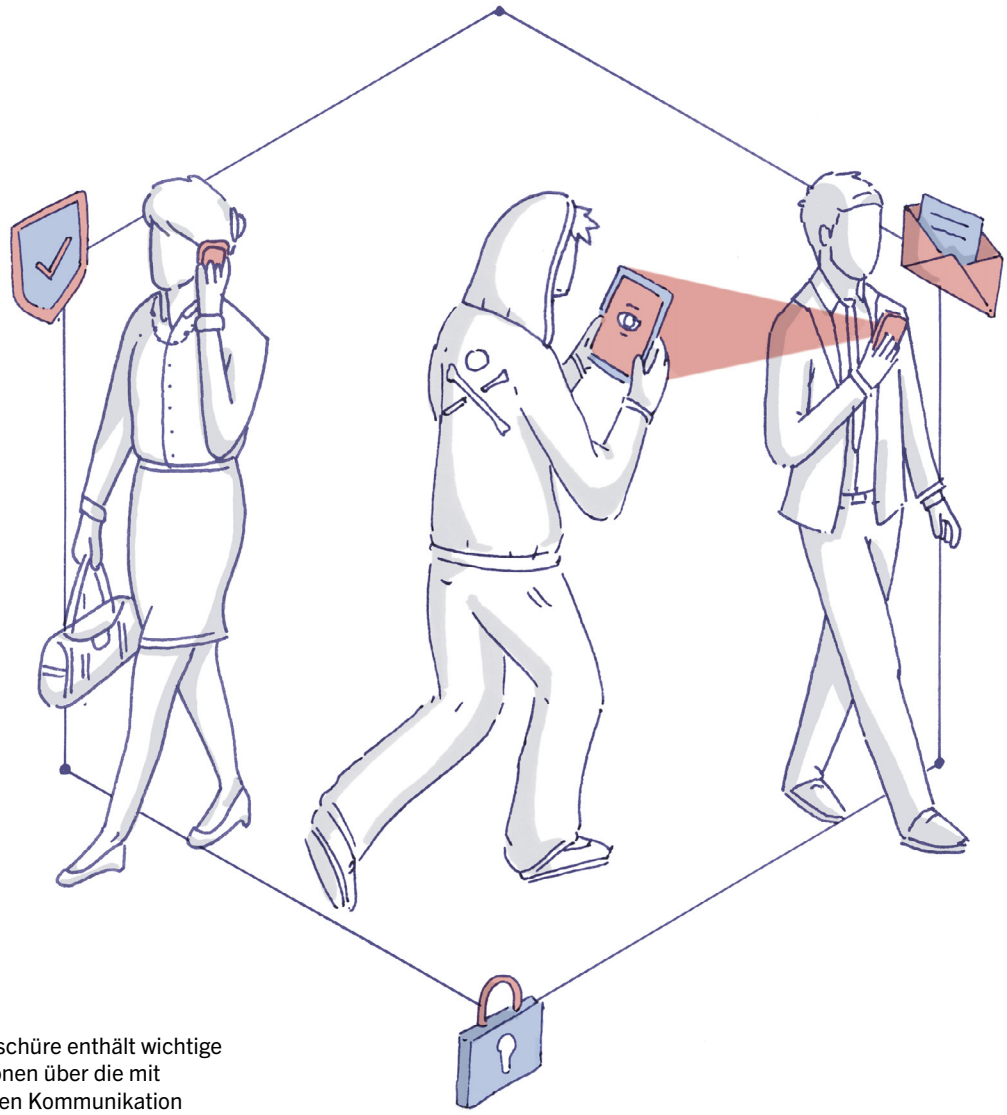
PICTET 1805

JANUAR 2020

CYBERSECURITY

SCHUTZ VOR DIGITALEN GEFAHREN



Diese Broschüre enthält wichtige Informationen über die mit der digitalen Kommunikation verbundenen Risiken und gibt den Leserinnen und Lesern ein paar einfache Tipps an die Hand, wie sie diese minimieren können.

PERSONENBEZOGENE DATEN: IMMER MEHR RISIKEN

Personenbezogene Daten sind heute ein wertvolles Gut. Mit ihnen können Gratisdienste wie soziale Netzwerke, Nachrichtensysteme oder öffentliche WLAN-Netze genutzt werden. Häufig wissen die Benutzerinnen und Benutzer jedoch wenig bis gar nichts über die Sicherheitsnormen, die diese Dienste zum Schutz ihrer Daten anwenden. Wer solche Daten sammelt, kann sie – ob legal oder illegal – kommerziell nutzen.

Bei der Übermittlung von personenbezogenen Daten ist daher absolute Vorsicht geboten, zumal Datendiebstahl unabhängig vom Benutzerverhalten immer häufiger wird. Auch Internetgiganten sind gegen Angriffe nicht gefeit: So wurden im Fall Cambridge Analytica die Daten von 87 Millionen Facebook-Nutzern entwendet und 2018 waren bei Google 52 Millionen Personen von einer Sicherheitslücke betroffen.

Das oberste Ziel von Pictet ist der Aufbau von partnerschaftlichen und verantwortungsvollen Geschäftsbeziehungen mit seinen Kundinnen und Kunden. Deren Schutz ist eines unserer Hauptanliegen – die Risiken für ihre personenbezogenen Daten bereiten uns deshalb Grund zur Sorge. Vor diesem Hintergrund haben wir diese Cybersecurity-Emp-fehlungen herausgegeben.

Personenbezogene Daten wie Identität, Lokalisierung oder Passwörter können leicht in die Hände von Kriminellen geraten, die damit auf Konten zugreifen oder ihre Opfer erpressen können. Mit ein paar einfachen Massnahmen lassen sich gewisse Risiken erheblich vermindern. In dieser Broschüre wird erläutert, wie die IT-Sicherheit verstärkt werden kann (s. Seite 4–5) und was im Falle von Datendiebstahl zu tun ist (s. Seite 6). Es empfiehlt sich, die Broschüre aufmerksam zu lesen und griffbereit aufzubewahren.

Januar 2020

WIE GEHEN HACKER VOR?

Durch das Sammeln vertraulicher Daten können Cyberkriminelle auf die Konten ihrer Opfer zugreifen oder diese erpressen.

Um an die personenbezogenen Daten ihrer Opfer heranzukommen, werden Hacker immer kreativer. Dabei reicht es manchmal, Informationen zu sammeln, die aus Nachlässigkeit oder Versehen veröffentlicht wurden. Sie können Passwörter oft auch einfach erraten, in Informatiksysteme eindringen oder sich für ihr Opfer ausgeben.

Cyberkriminelle arbeiten vielfach mit Mitteilungen, in denen alarmierende Situationen beschrieben werden („Ihr Computer hat einen Virus“) oder die an das Mitgefühl appellieren („ein Freund befindet sich in einer schwierigen Lage“), dringendes Handeln erfordern („Ihre rasche Reaktion ist gefragt“) oder finanzielle Gewinne in Aussicht stellen („eine einmalige Gelegenheit“).

Hier einige Beispiele von Datendiebstahl bzw. Betrugsfällen:

1.DER TEUFEL STECKT IM DETAIL

In einem E-Mail eines bekannten Absenders wird ein Benutzer dazu aufgefordert, eine Nachahmung der Pictet-Website zu besuchen, deren URL dem Original zum Verwechseln ähnlich ist, wie zum Beispiel picttet.com, pIctet.com oder pic-tet.com. Durch diesen Trick können Cyberkriminelle an die Daten der Opfer gelangen und diese anschliessend weiterverwenden.

2.DATEN IN GEISELHAFT

Eine Benutzerin erhält ein E-Mail von einer Person, deren Identität gestohlen wurde. Durch Öffnen des darin enthaltenen Anhangs wird der Computer des Opfers gesperrt. Eine Mitteilung erscheint auf dem „Sperrbildschirm“, mit der das Opfer aufgefordert wird, Lösegeld auf ein Kryptokonto einzuzahlen, damit der Computer wieder entsperrt wird. In den Medien wird über solche Erpressungsmethoden häufig unter dem Begriff „Ransomware“ berichtet.

3.CEO-BETRUG

Ein Angestellter der Buchhaltung erhält einen Anruf einer Cyberkriminellen, die sich für seine Vorgesetzte oder eine hochrangige Führungskraft ausgibt. Unter Vorgabe einer dringenden Angelegenheit (Kauf im Ausland, Steuerprüfung usw.) verlangt sie die Offenlegung von vertraulichen Daten.

SICHERHEITSTIPPS UND VERHALTENSREGELN

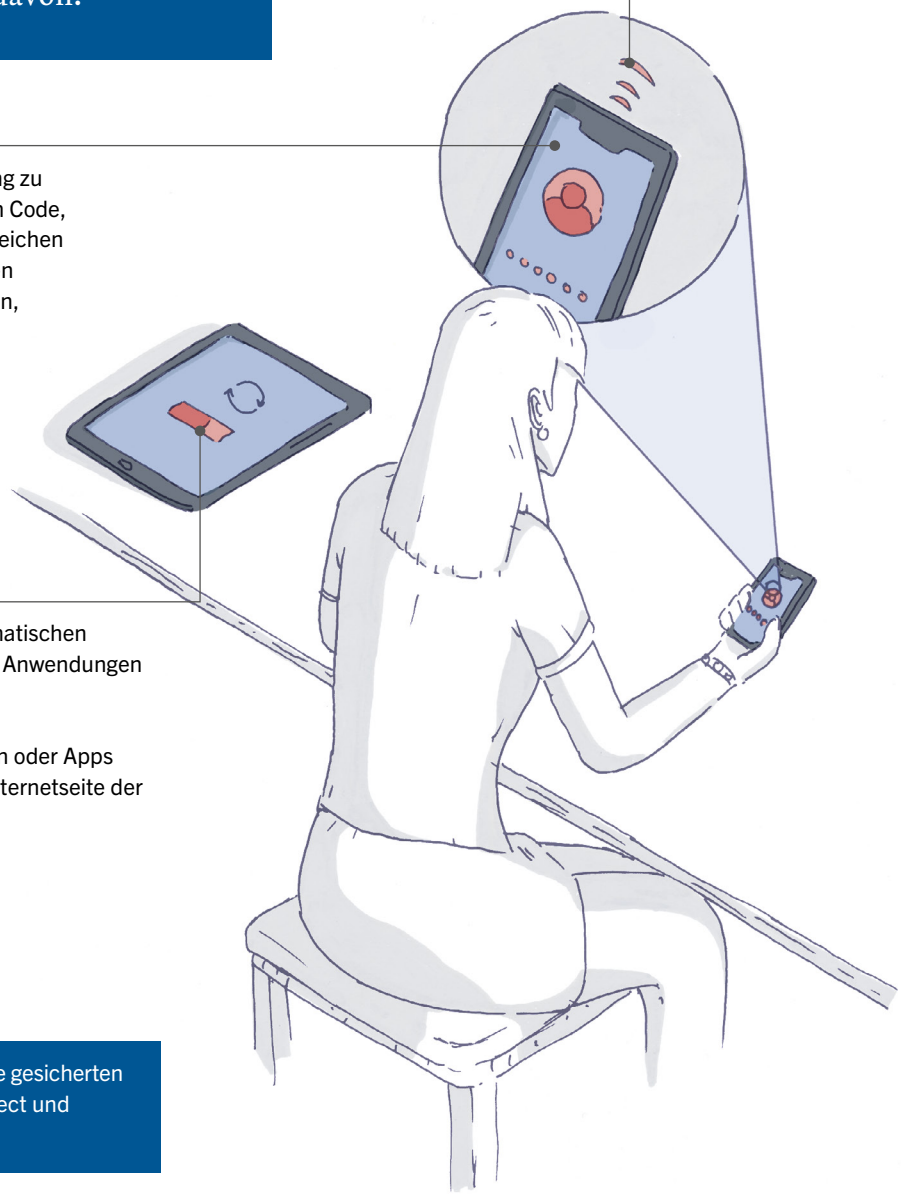
Es gibt viele einfache Massnahmen, um sich vor Datendiebstahl und Betrug zu schützen. Hier sind einige davon.

Aktivieren Sie die Optionen, mit denen die Daten auf einem gestohlenen oder verlorenen Gerät aus der Ferne gelöscht werden können.

Bewahren Sie keine vertraulichen Informationen (Passwörter, Daten zu Finanztransaktionen usw.) in Ihrer Mailbox auf.

Schützen Sie den Zugang zu Ihren Geräten mit einem Code, der mindestens sechs Zeichen umfasst, oder verwenden Sie biometrische Sperren, die genauso sicher sind.

Desaktivieren Sie nie Schutzmechanismen (z.B. den PIN-Code).



Aktivieren Sie die automatischen Update-Funktionen von Anwendungen und Apps.

Laden Sie Anwendungen oder Apps nur von der offiziellen Internetseite der Hersteller herunter.

Bevorzugen Sie in jedem Fall die gesicherten Kanäle von Pictet (Pictet Connect und mobile Apps).

Überprüfen Sie die Adressen der Websites, die Sie besuchen.

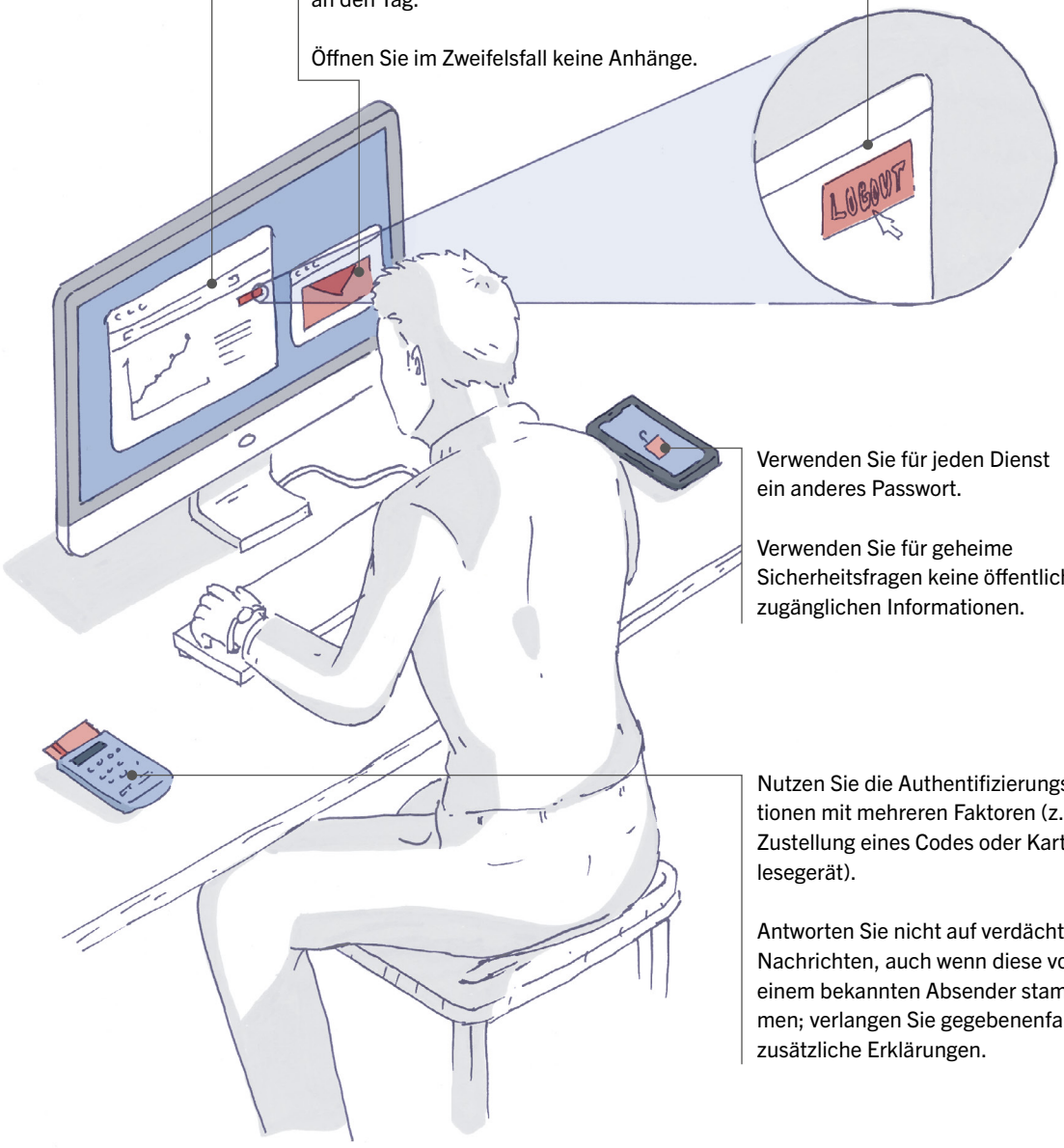
Legen Sie auf nicht gesicherten Websites keine Informationen offen, insbesondere wenn Sie an ein öffentliches Netzwerk angeschlossen sind.

Legen Sie ein gesundes Misstrauen gegenüber unaufgeforderten E-Mails an den Tag.

Öffnen Sie im Zweifelsfall keine Anhänge.

Schliessen Sie Sitzungen stets über die dafür vorgesehenen Funktionen.

Lassen Sie Ihre Sitzung nie unbeaufsichtigt, solange sie offen ist.



Verwenden Sie für jeden Dienst ein anderes Passwort.

Verwenden Sie für geheime Sicherheitsfragen keine öffentlich zugänglichen Informationen.

Nutzen Sie die Authentifizierungsoptionen mit mehreren Faktoren (z. B. Zustellung eines Codes oder Kartenlesegerät).

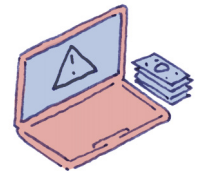
Antworten Sie nicht auf verdächtige Nachrichten, auch wenn diese von einem bekannten Absender stammen; verlangen Sie gegebenenfalls zusätzliche Erklärungen.

WAS TUN BEI DATENDIEBSTAHL?

Im Schadensfall sind umgehend folgende Massnahmen zu ergreifen.

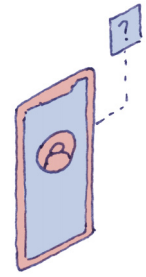
MEIN E-MAIL-KONTO WURDE GEHACKT

- Setzen Sie den Zugang mithilfe der Betriebsangaben zurück und ändern Sie umgehend das Passwort (dies gilt für alle Konten, für die Sie dasselbe Passwort benutzen).
- Informieren Sie Nahestehende und Ihre Kontakte, dass die betroffene E-Mail-Adresse vorläufig nicht sicher ist.
- Schätzen Sie aufgrund des Inhalts der Mailbox (Informationen zu Transaktionen, vertrauliche Daten usw.) ein, wie gross der potenzielle Schaden sein könnte und kontaktieren Sie die betroffenen Personen.
- Überprüfen Sie die Einstellungen der Mailbox (bzw. lassen Sie diese überprüfen), insbesondere im Hinblick auf die Option zum automatischen Weiterleiten von Nachrichten, die von den Hackern möglicherweise eingerichtet wurde.



ICH WERDE DIGITAL ERPRESST

- Gehen Sie nicht auf Lösegeldforderungen ein.
- Wenden Sie sich umgehend an eine/n IT-Experten/in.



ICH HABE SENSIBLE INFORMATIONEN PER TELEFON AN EINE PERSON MIT BÖSWILLIGEN ABSICHTEN WEITERGEGEBEN

- Ändern Sie alle möglicherweise betroffenen Passwörter.
- Informieren Sie alle möglicherweise betroffenen Geschäftspartner und Nahestehenden.
- Sperren Sie die Telefonnummer der Täterin bzw. des Täters und antworten Sie auf keine weiteren Anfragen.

WORAN ERKENNT MAN EINE BETRUGSNACHRICHT?

Zwar gibt es keine hundertprozentig sichere Methode, um betrügerische Absichten zu erkennen, doch auf einige Warnsignale sollten Benutzerinnen und Benutzer besonders achten.

Ihr Misstrauen wecken sollten Nachrichten, die:

- von einer unbekannten oder ungewohnten Adresse aus verschickt wurden; Achtung: Cyberkriminelle versuchen häufig, Adressen von bekannten Kontakten nachzuahmen;
- verdächtige Elemente beinhalten, einen bedrohlichen Ton aufweisen oder zu dringendem Handeln auffordern;
- vage oder eigenartige Versprechen enthalten;
- dazu auffordern, einen Anhang zu öffnen oder auf einen Link zu klicken, damit der gesamte Inhalt der Nachricht angezeigt wird;
- den Empfänger der Nachricht nicht direkt ansprechen und nicht die übliche Absenderadresse verwenden.

Auch wenn eine Nachricht eine oder mehrere der genannten Merkmale aufweist, heisst das nicht unbedingt, dass es sich um eine Betrugsmail handelt. In jedem Fall sind jedoch Sicherheitsvorkehrungen geboten, bevor das E-Mail bearbeitet wird.

Pictet
Die Pictet-Gruppe ist ein von derzeit sieben Teilhabern geführtes Unternehmen, dessen Grundsätze bezüglich Eigentumsübertragung und Nachfolgeregelung sich seit der Gründung im Jahr 1805 nicht verändert haben. Sie ist ausschliesslich in den Bereichen Wealth Management, Asset Management und Asset Services tätig, betreibt kein Investmentbanking und ist nicht im Kreditgeschäft aktiv. Mit verwalteten oder verwahrten Vermögen von CHF 544 Mrd. per 30. Juni 2019 zählt Pictet heute zu den führenden unabhängigen Vermögensverwaltern Europas für Privatkunden und institutionelle Anleger.

Die Gruppe hat ihren Hauptsitz in Genf, Schweiz, wo sie gegründet wurde, beschäftigt über 4300 Personen und hat weltweit insgesamt 27 Geschäftsstellen in: Amsterdam, Barcelona, Basel, Brüssel, Dubai, Frankfurt, Genf, Hongkong, Lausanne, London, Luxemburg, Madrid, Mailand, Montreal, München, Nassau, Osaka, Paris, Rom, Singapur, Stuttgart, Taipeh, Tel Aviv, Tokio, Turin, Verona und Zürich.

Realisation
Large Network

FSC
MIX
Paper
FSC® C002504

www.gruppe.pictet