Ratgeber

Sicheres Banking.

Zürcher Kantonalbank

Bitte beachten Sie, dass es sich bei den in diesem Ratgeber behandelten Themen lediglich um eine Auswahl handelt, die weder vollständig ist, noch ersetzt sie die einzelnen Produktverträge und -bestimmungen sowie die dort geregelten Risikohinweise, empfohlenen Sicherheitsvorkehrungen und Sorgfaltspflichten des Kunden, die vorrangig beachtet werden müssen.

Tipps für ein sicheres Banking.

Liebe Kundin, lieber Kunde

Sicherheit und Banken gehören seit jeher eng zusammen. Und genauso alt wie Banken sind kriminelle Versuche, deren Sicherheitsmassnahmen zu unterlaufen. Früher waren es bewaffnete Banden, die mit spektakulären Banküberfällen grosse Schäden anrichteten. Später Scheckbetrüger, die sich unrechtmässig bereicherten.

Mit der Digitalisierung hat die Cyberkriminalität Einzug gehalten. Neben Gold und Bargeld sind nun auch Daten und Informationen im kriminellen Fokus. Schon immer war die Zürcher Kantonalbank bestrebt, auch die neuesten Tricks der Angreifer mit wirkungsvollen Schutzmassnahmen zu vereiteln. Wir verbessern unsere Systeme und Überwachungsmethoden laufend und passen unsere Abwehrdispositive den jeweils aktuellen Bedrohungen an. Zum Schutz Ihrer Daten erfüllen wir hohe Sicherheitsstandards.

Auch Sie können sich gegen Betrug und Diebstahl wehren. In diesem Ratgeber geben wir Ihnen Tipps, wie Sie betrügerische Absichten in der digitalen und analogen Welt besser erkennen und sich davor schützen können.

Remo Schmidli
Leiter IT, Operations & Real Estate
Mitglied der Generaldirektion
Zürcher Kantonalbank

Inhalt

Editorial

Bankgeschäfte verlagern sich immer weiter in die elektronische Welt.

Zunehmende Digitalisierung

Bankgeschäfte und Zahlungsverkehr verlagern sich immer weiter in die elektronische Welt. Die technologische Entwicklung ist unaufhaltsam und die Vielfalt der Möglichkeiten nimmt laufend zu. Hier den Überblick zu behalten, ist nicht immer leicht. Trotzdem ist es nicht so schwierig, sich sicher in der elektronischen Welt zu bewegen: Wenn Sie sich an die folgenden Tipps halten, ist schon ein grosser Schritt getan.

Die wichtigsten fünf Tipps für sicheres Banking

1. Geben Sie niemals persönliche Daten wie Vertragsnummer, Passwort oder PIN (Persönliche Identifikations-Nummer) preis – weder am Telefon noch im Internet.
2. Identifizieren Sie am Telefon ob es sich z.B. tatsächlich um einen Mitarbeitenden der Bank handelt.
3. Prüfen Sie die Herkunft unerwarteter E-Mails und öffnen Sie bei Verdacht keine Links oder Anhänge.
4. Lassen Sie sich am Bancomat nicht ablenken und schauen Sie, ob dieser manipuliert sein könnte.
5. Sperren Sie Ihr Konto und Ihre Karte bei Verdacht.

Worauf Sie sonst noch achten sollten, erfahren Sie auf den nächsten Seiten.

Bitte beachten Sie, dass es sich bei den in diesem Ratgeber behandelten Themen lediglich um eine unvollständige Auswahl handelt. Sie ersetzen nicht die einzelnen Produktverträge und -bestimmungen oder die dort geregelten Risikohinweise. Darin empfohlene Sicherheitsvorkehrungen und Sorgfaltspflichten auf Kundenseite sind vorrangig zu beachten.

ZKB Apps für mobile Geräte

Mobile Nutzung verschiedener Bankdienstleistungen.

Die Zürcher Kantonalbank bietet zur mobilen Nutzung verschiedener Bankdienstleistungen diverse Apps an. Mit der zunehmenden Verbreitung mobiler Geräte wie Smartphones oder Tablets, steigt auch die Attraktivität für Angriffe auf Mobile-Banking-Apps. Mit den folgenden Hinweisen gestalten Sie den Umgang mit den ZKB Apps sicherer:

– Stellen Sie sicher, dass Sie immer die offiziellen Apps der Zürcher Kantonalbank auf Ihrem mobilen Gerät installieren. Diese offiziellen ZKB Apps finden Sie unter zkb.ch/digitales-banking.
– Installieren Sie die ZKB Apps immer vom offiziellen App Store (iOS) oder Play Store (Android). Installieren Sie keine Apps aus Ihnen unbekannten, nicht vertrauenswürdigen Quellen.
– Aktivieren Sie immer einen Sperrcode für Ihr mobiles Gerät.
– Aktualisieren Sie Ihre Geräte immer auf die neuste verfügbare Version des Betriebssystems.
– Installieren Sie Betriebssystem-Updates umgehend.

Mobiles Gerät verloren?

Sie haben Ihr mobiles Gerät mit den ZKB Apps verloren oder es wurde Ihnen gestohlen? Sperren Sie Ihr eBanking über den eBanking Support (0844 840 140) oder loggen Sie sich mit der richtigen Vertragsnummer im Browser ein und setzen Sie fünfmal ein falsches Passwort. Dadurch wird Ihr eBanking automatisch gesperrt und ist vor Zugriff geschützt.

eBanking

Zahlen Sie bequem online.

eBanking ist gut geschützt
Mit eBanking erledigen Sie Ihre Bankgeschäfte bequem online. Unsere eBanking-Dienstleistungen erfüllen strenge Sicherheitsnormen und wir lassen diese regelmässig durch unabhängige externe Sicherheitsexperten überprüfen.

Tipps und Hinweise

Phishing erkennen
Finanzinstitute werden Sie nie per E-Mail oder telefonisch nach persönlichen Daten wie Vertragsnummer, Passwort, TAN oder Telefonnummer fragen.

Hinterfragen Sie jede eingehende E-Mail kritisch. Erwarte ich eine Sendung? Kenne ich den Absender? Fragen Sie im Zweifelsfall telefonisch beim Absender nach. Klicken Sie nie auf einen Anhang oder einen Link in einer E-Mail, wenn Sie dieser nicht 100 Prozent vertrauen.

Sorgfältig handeln
Seien Sie vorsichtig mit Ihren persönlichen Daten und geben Sie diese nicht unbedacht auf Webseiten ein.

Geschützt speichern
Speichern Sie Ihre Zugangsdaten in einem Passwort-Manager.

Warnungen beachten
Beachten Sie die Sicherheitshinweise, die gelegentlich beim Einloggen ins eBanking angezeigt werden. Dort informieren wir Sie über aktuelle Risiken.

Auf den Webseiten zkb.ch/sicherheit und ebas.ch (eBanking – aber sicher) finden Sie weitere Informationen für sicheres eBanking. «eBanking – aber sicher!» ist eine unabhängige Plattform der Hochschule Luzern, die Sie dabei unterstützt, Ihre persönliche Informationssicherheit zu wahren. Die Zürcher Kantonalbank ist Partnerin dieser Plattform.

Karten

Mit der Karte bequem und sicher bezahlen.

Wenn Sie Bargeld verlieren, ist es weg. Ihre Karte können Sie umgehend sperren lassen.
Kartenzahlungen sind aus dem Alltag nicht mehr wegzudenken. Viele Karten bieten heute zusätzlich die Möglichkeit, Zahlungen bis CHF 80 kontaktlos und ohne PIN-Eingabe abzuwickeln. So einfach geht's: Karte ans Bezahl-Terminal halten – fertig. Auf unseren Karten ist ein Chip der neuesten Generation im Einsatz. Er erlaubt nicht nur kontaktloses Bezahlen, sondern ist auch in punkto Sicherheit auf dem neusten Stand. Ab CHF 80 muss bei kontaktlosen Transaktion immer die PIN eingegeben werden. Nach dem Zufallsprinzip wird sie aus Sicherheitsgründen gelegentlich auch bei Beträgen unter CHF 80 abgefragt. Kontaktlos bezahlen können Sie überall dort, wo Sie das Kontaktlos-Symbol sehen.

Kriminelle versuchen auf verschiedenen Wegen Karten und Kartendaten zu stehlen. In den meisten Fällen bleibt es beim Versuch. Erscheint uns eine Kartentransaktion nicht plausibel, setzen wir uns mit Ihnen in Verbindung. Haben Sie selbst den Verdacht, dass Ihre Karte missbraucht wird, lassen Sie sie unverzüglich sperren.

Tipps und Hinweise

Karte unterschreiben
Unterschreiben Sie Ihre Karten sofort bei Erhalt auf der Rückseite. Vernichten Sie Ihre alte Karte, indem Sie den Magnetstreifen und den Chip der Karte zerschneiden.

PIN anpassen
Ändern Sie die PIN, die Sie von uns erhalten haben, an einem Bancomat in eine gut merkfähige vier- bis sechsstellige Zahlenkombination. Verwenden Sie keine naheliegenden Kombinationen wie Geburtsdatum, Telefon- oder Autonummer oder den Sperrcode Ihres Mobiltelefons.

PIN merken

Bewahren Sie Ihre PIN ausschliesslich in Ihrem Gedächtnis und keinesfalls schriftlich zusammen mit Ihrer Karte auf. Die PIN Ihrer Maestro-, ZKB-Kontokarte oder Kreditkarte können Sie am Bancomat beliebig ändern.

Sorgfältig aufbewahren

Bewahren Sie Ihre Karte sorgfältig auf und geben Sie sie niemandem weiter.

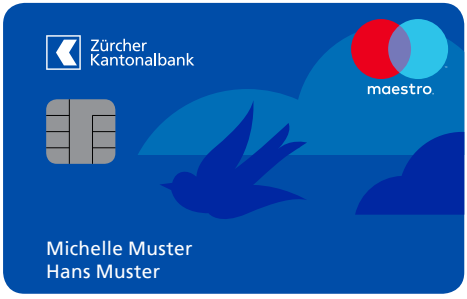
Karte sperren

Lassen Sie Ihre Karte bei Verlust, Verdacht auf Missbrauch oder wenn sie in einem Automaten stecken bleibt sofort sperren. Alle wichtigen Telefonnummern dazu finden Sie am Ende dieser Broschüre. Oder sperren Sie Ihre Maestro- oder Kontokarte gleich selbst und kostenlos im eBanking oder eBanking mobile respektive Ihre Kredit- oder PrePaidkarte in der one App.

Sichere Verfahren nutzen

Achten Sie beim Bezahlen mit der Kreditkarte im Internet darauf, dass die Übermittlung der Daten verschlüsselt erfolgt (siehe auch Kapitel Computer und Internet). Nutzen Sie bei Einkäufen im Internet für zusätzliche Sicherheit das sogenannte 3D-Secure-Verfahren. Damit bestätigen Sie Ihre Transaktion erneut via Smartphone-App.

Ob Ihre Karte kontaktlos bezahlen kann, erkennen Sie an diesem Symbol.



Geldautomat

Schauen Sie genau hin und achten Sie auf die Umgebung.

Lassen Sie sich nicht ablenken

Täter versuchen häufig die Person am Geldautomaten auf eine dreiste Weise abzulenken. Sie greifen ins Tastenfeld oder entwenden das Bargeld, wenn es aus dem Automaten kommt. Lassen Sie sich vor, während und nach einem Bargeldbezug nicht von Fremden ansprechen oder mit Fragen ablenken. Achten Sie auf Personen in der Umgebung, die sich merkwürdig verhalten und melden Sie diese der Polizei oder dem Personal in der Filiale.

Geldautomaten können manipuliert werden

Täter versuchen immer wieder, Geldautomaten oder Zahlterminals wie zum Beispiel Billettautomaten zu manipulieren, damit sie eine Karte unbemerkt kopieren können. Häufig sind die Manipulationen mit blossem Auge kaum zu erkennen. Um die gestohlene oder kopierte Karte erfolgreich einzusetzen, benötigen die Täter aber zusätzlich zur Karte die PIN.

Tipps und Hinweise

Geldautomat, Ticketautomat, Tankomat und Zahlautomat prüfen

Schauen Sie sich den Automaten an und untersuchen Sie, ob bewegliche Gegenstände oder ungewöhnliche Abdeckungen daran angebracht sind.

Polizei informieren

Haben Sie den Verdacht, dass ein Automat manipuliert wurde, so informieren Sie bitte umgehend die Polizei (Telefon 117).

PIN verdeckt eingeben

Achten Sie darauf, dass Sie Ihre PIN immer verdeckt eingeben. Verwenden Sie dazu Ihre zweite Hand oder das Portemonnaie.

Nicht ablenken lassen

Beachten Sie Personen, die sich Ihnen beim Bargeldbezug nähern. Brechen Sie gegebenenfalls den Vorgang ab und bestehen Sie auf Ihre Privatsphäre. Das gilt auch für den Einsatz der Karte an einer Kasse. Ändern Sie im Zweifelsfall an einem anderen Geldautomaten möglichst schnell Ihre PIN.

Karte nicht aus der Hand geben

Geben Sie Ihre Karte nie aus der Hand – weder einem vermeintlichen Helfer beim Geldautomaten noch einem Serviceangestellten. Die Karte kann blitzschnell ausgetauscht werden, ohne dass Sie es merken.

Als Skimming wird das illegale Ausspähen von Kartendaten und das Kopieren des Magnetstreifens bezeichnet. Dazu werden Geldautomaten oder auch andere Zahlstellen wie Tank- oder Billettautomaten manipuliert. Mehr dazu auf der Webseite der Kantonspolizei (stop-skimming.ch) oder auf der Webseite Kriminalprävention CH (skppsc.ch/de/themen/betrug/skimming).

Betrugsarten

Nicht nur ältere Personen sind betroffen: auch jüngere Personen geraten in die Fänge von Betrügern.

Betrüger sind Meister ihres Faches, die sehr überzeugend und bestimmt auftreten und nur schwer durchschaubar sind. Die Betrugsarten sind sehr vielfältig, weshalb nachstehende Beispiele nicht abschliessend sein können. Wenn Sie einen Betrugsfall vermuten, wenden Sie sich an Ihren Kundenbetreuer.

Enkeltrickbetrug/
Betrug mit falschen Polizisten
Häufig beginnt ein Trickbetrug mit einem Telefonanruf des Betrügers. Dies ist praktisch in allen Fällen von Enkeltrickbetrug oder Betrug mit falschen Polizisten der Fall.

Beim Enkeltrickbetrug nutzen die Betrüger die Hilfsbereitschaft der Opfer mit einer glaubwürdigen Geschichte zu einer angeblichen finanziellen Notlage aus. Das Opfer, das mit einem vermeintlichen Verwandten spricht, fühlt sich verpflichtet zu helfen und wird dadurch unter Druck gesetzt. Die angerufene Person wird so manipuliert, dass sie Geld abhebt und es dann fremden Personen übergibt.

Beim Trick mit den falschen Polizisten sind ebenfalls professionelle Kriminelle am Werk. Sie rufen die Opfer an und erzählen ihnen eine Geschichte über einen angeblichen kriminellen Vorfall in ihrem Umfeld, der sie in Angst und Schrecken versetzt. Gleichzeitig wird das Opfer massiv unter Druck gesetzt, sich keinem Dritten anzuvertrauen. Die vermeintliche Polizei bittet das Opfer um Mithilfe, die angeblich zur Ergreifung der Täterschaft notwendig sei. Die Opfer werden genötigt, einem «Polizisten» Vermögenswerte zu übergeben oder aber Geld direkt via eBanking bei der angeblichen Polizei in Sicherheit zu bringen.

Mehr zu diesen Themen erfahren Sie auf einer Webseite der Kantonspolizei Zürich: telefonbetrug.ch.

Romance-Scam (Liebesbetrug)
Social Media (Facebook etc.) und zunehmende Vereinzelung gefährden immer mehr Personen, unabhängig von Alter und Geschlecht, zu Opfern von sogenannten Liebesbetrügern zu werden. Mit gefälschten Identitäten/Profilen gelingt es den Betrügern, eine scheinbare Liebesbeziehung zu den Opfern aufzubauen. Schon bald fordern sie wegen einer angeblichen Notsituation Geld. Dem Opfer wird versprochen, dass der geliehene Betrag schnell wieder zurückbezahlt wird, was jedoch nicht geschieht. Zunehmende emotionale Abhängigkeit führt zu immer weiteren Geldforderungen. Die angebliche Liebesbeziehung dient einzig der finanziellen Bereicherung der jeweiligen Betrüger. Für Dritte, also Angehörige, Freunde, die Bank etc., ist es sehr schwierig, die Opfer von einem Betrug zu überzeugen, da sie emotional stark involviert sind.

Im Internet finden sich viele derartige Geschichten. Wir empfehlen einen Besuch von skppsc.ch/de/themen/internet/romance-scam der Kriminalprävention Schweiz.

Investment-Betrug

Investment-Betrüger locken trotz anhaltend niedrigen Zinsumfeldes mit hohen Renditen.

Den Betrügern gelingt es, die Opfer glauben zu machen, rascher Gewinn sei möglich. Um sie davon zu überzeugen und weiter in die Falle zu locken, werden manchmal auch kleinere Beträge als Zinsen ausbezahlt. Die somit in ihrem Vertrauen bestärkten Opfer tätigen dann weitere Investitionen, oft über einen längeren Zeitraum. Schliesslich haben Opfer oft sehr viel investiert. Wenn Sie dann irgendwann aussteigen wollen, wird suggeriert, dass dies – gerade jetzt! – ohne Verlust nicht möglich sei. Weitere Investitionen könnten aber helfen diesen Verlust zu vermeiden usw. Die Formen des Investment-Betruges sind sehr vielseitig.

Beim Nationalen Zentrum für Cybersicherheit finden Sie weitere Informationen: ncsc.admin.ch/ncsc/de/home/cyberbedrohungen/investmentbetrug.

CEO-Betrug

Immer wieder richten gefälschte E-Mails, die vorgeben von einem Kaderangestellten oder gar dem Chef der eigenen Firma zu sein, grosse Schäden an. In diesen gefälschten E-Mails geht es immer um eine dringende, oft auch vertrauliche Angelegenheit. Schliesslich überweist der pflichtbewusste Mitarbeitende im guten Glauben es im Auftrag der Leitung zu tun grosse Summen ins Ausland. Wenn der Betrug auffällt, ist es meistens schon zu spät. Wenn Ihre Firma Opfer eines solchen Betruges wurde, zählt jede Minute. Rufen Sie unverzüglich Ihren Kundenberater an und schildern Sie den Betrug.

Im Internet hat es viele Beispiele von Fällen. Weitere Informationen finden Sie zum Beispiel bei der Kriminalprävention Schweiz (skppsc.ch/de/der-ceo-fraud-in-vier-schritten-erklaert).

Betrug mit gefälschten Zahlungsinstruktionen von bekannten Lieferanten

Eine weitere verbreitete Betrugsart ist der sogenannte «Lieferantenbetrug». Firmen erhalten oft in Form eines gehackten E-Mails von langjährigen Lieferanten aus dem Ausland die Mitteilung, dass sich deren Bankverbindungen (Angaben für Einzahlungen) geändert hätten. Dadurch werden die Rechnungen auf die neue Bankverbindung einbezahlt. Es vergeht oftmals längere Zeit, bis sich der Lieferant meldet und fragt, warum die Rechnung nicht bezahlt wurde. Erst dann fällt der Betrug auf. Die von der Täterschaft angegebenen neuen Kontoverbindungen lauten ebenfalls auf den Namen der Lieferanten. Wir empfehlen: Wenn Sie von Lieferanten, besonders aus dem Ausland, eine Mitteilung zur veränderten Bankverbindung erhalten, fragen Sie auf einem anderen Kanal, z.B. Telefon zurück, ob dies tatsächlich der Fall ist.

Falschgeld

Trotz hoher Sicherheitsstandards werden immer noch gefälschte Banknoten in Umlauf gebracht. Das meiste Falschgeld wird bei Banken, Geschäften oder auch bei Werttransporten entdeckt. Gefälschte Banknoten müssen in der Schweiz der Polizei übergeben werden. Besonders ist aber auch im Ausland Vorsicht geboten, da man in der Regel mit fremden Noten nicht sehr vertraut ist.

Informieren Sie sich über die Sicherheitsmerkmale von Schweizer Franken auf der Webseite der Schweizerischen Nationalbank snb.ch oder für Euronoten bei der Europäischen Zentralbank ecb.europa.eu.

Computer und Internet

Sichern – Schützen – Überwachen – Vorbeugen – Aufpassen.

Sichern

Ihre Daten sind wertvoll

Die Wiederherstellung elektronischer Daten ist mühsam und zeitaufwändig.

Tipps und Hinweise

Daten sichern

Sichern Sie wichtige Dokumente, E-Mails und andere elektronische Daten regelmässig auf einem externen Datenträger (USB-Stick, externe Festplatte, DVD, CD) oder online. Je wichtiger die Daten sind, desto häufiger sollten Sie eine Sicherungskopie erstellen.

Backup prüfen

Kontrollieren Sie, ob Ihre Daten vollständig gespeichert wurden und prüfen Sie, ob die Daten wiederhergestellt werden können.

Festplatte ausstecken

Schliessen Sie einen externen Datenträger nur dann an den Computer an, wenn Sie ihn benötigen. So reduzieren Sie die Gefahr eines Befalls durch Schadsoftware (Malware).

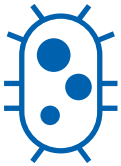
Sicheres Löschen

Denken Sie daran, dass gelöschte Daten wiederherstellbar sind. Konsultieren Sie einen IT-Spezialisten für eine endgültige Löschung persönlicher Daten, bevor Sie ein Gerät entsorgen, weitergeben oder weiterverkaufen.

Schützen

Einsatz eines Virenschutzprogrammes

Ohne speziellen Schutz ist ein Computer (PC, Notebook, Smartphone, Tablet, etc.) den Gefahren im Internet schutzlos ausgeliefert und kann mit Schadsoftware infiziert werden.



Tipps und Hinweise

Viren- und Malwareschutzprogramm installieren

Nutzen Sie Programme, die Ihren Computer laufend auf Viren und Malware überprüft. Installieren Sie aber keinesfalls mehrere solcher Programme, da sich diese gegenseitig neutralisieren können.

Regelmässig aktualisieren

Konfigurieren Sie das Virenschutzprogramm so, dass es sich automatisch aktualisiert.

System scannen

Prüfen Sie Ihren Computer regelmässig auf Schadsoftware. Insbesondere nach dem Herunterladen grosser Datenmengen aus möglicherweise unsicheren Quellen: Lassen Sie dazu das Virenschutzprogramm das komplette System scannen (vollständige Systemprüfung).

Anhänge prüfen

Prüfen Sie Dateianhänge in E-Mails vor dem Öffnen mit Hilfe eines Virenschutzprogrammes auf mögliche Schadsoftware.

Überwachen

Einsatz einer Firewall

Wenn Sie mit Ihrem Computer im Internet surfen, öffnen sich auf den Geräten unsichtbare «Zugangstüren» (Ports). Diese bieten eine Angriffsfläche für Attacken aus dem Internet. Eine Firewall schliesst diese Türen soweit wie nötig und überwacht den Datenverkehr vom und zum Internet. Die Firewall alarmiert Sie, wenn verdächtiger Internetverkehr entdeckt wird.

Tipps und Hinweise

Firewall aktivieren

Wenn Ihr Computer über eine Firewall verfügt, so aktivieren Sie diese unbedingt, bevor Sie ihn mit dem Internet verbinden. Oft werden Firewalls gemeinsam mit dem Antivirenprogramm erworben.

Sicher downloaden

Laden Sie Software-Updates und Programme nur herunter, wenn Ihre Firewall aktiviert ist.

Nicht alle Türen öffnen

Gewisse Onlineprogramme wie zum Beispiel Onlinespiele verlangen das Öffnen bestimmter «Zugangstüren» (Ports). Konsultieren Sie hierzu unbedingt einen IT-Spezialisten, damit nur die wirklich erforderlichen Zugänge geöffnet werden und nicht die ganze Firewall deaktiviert wird.

Besondere Hinweise für Unternehmerinnen und Unternehmer

Content-Filter aktivieren

Benutzer greifen täglich auf das Internet zu, um ihre Arbeit zu erledigen. Ein

Content-Filter überwacht den Internet-Verkehr und blockiert schädlichen Inhalt oder schädliche Webseiten, bevor diese am Arbeitsplatz des Benutzers ausgeführt werden.

Privilegierte Benutzeraccounts einschränken

Benutzer mit Administratorenrechten oder Benutzer mit erhöhten Rechten bergen Risiken für das Unternehmen, da diese Rechte oft von Cyberkriminellen ausgenutzt werden. Administratorenrechte sollten daher äusserst restriktiv vergeben werden. Darüber hinaus sind derartige Benutzer-Accounts besonders zu überwachen.

Sicherheitsupdates

Veraltete Software ist ein beliebtes Einfallstor für Schadsoftware. Stellen Sie sicher, dass sämtliche Computer und Server in Ihrem Netzwerk Sicherheitsupdates automatisch einspielen (Aktivierung automatischer Updates). Patchen Sie Drittsoftware, wie z. B. Adobe Reader, Adobe Flash, Java, ebenfalls regelmässig. Das gilt auch für die Treiber der eingesetzten Hardware wie Drucker, Router usw.

Log Management System einsetzen

Ein Log Management System ermöglicht es einem Administrator zu prüfen, ob ein Angreifer unbemerkt in ein Computersystem eindringen konnte. Dabei werden Logfiles aus diversen Applikationen gesammelt und korreliert. Intelligente Auswertungsfunktionen helfen dabei, die gewünschte Information auf einfache Weise zu finden.

Intrusion Detection System implementieren

Ein Intrusion Detection System erkennt aufgrund anpassbarer, definierter Regeln Angriffe auf Computersysteme oder Netzwerke. Die eingebaute Alarmierungsfunktion informiert den Administrator umgehend über den Eindringversuch, damit entsprechende Gegenmassnahmen eingeleitet werden können.

Vorbeugen

Aktualisieren Sie Ihren Computer regelmässig

Wer im Internet surft, sollte immer mit der neuesten Version des Browsers, des Virenschutzprogrammes sowie des Betriebssystems unterwegs sein. Veraltete Programme haben oft Sicherheitslücken. Diese vereinfachen es einem Angreifer, einen Computer unter seine Kontrolle zu bringen. Aus diesem Grund bieten Hersteller regelmässig Updates an. Das ist wichtig, weil immer wieder neue Angriffsmethoden von Cyberkriminellen bekannt werden oder neue Schadsoftware im Umlauf ist.

Tipps und Hinweise

Automatisch updaten

Aktivieren Sie die automatische Updatefunktion für alle installierten Programme und Apps (insbesondere Betriebssystem, Virenschutzprogramm, Firewall, Browser).

Browser aktualisieren

Verwenden Sie für den Zugang ins Internet nur die jeweils aktuellste Version des Browsers.

Quellen prüfen

Installieren Sie keine Programme von Anbietern, die Sie nicht kennen. Oft enthält kostenlose Software auch Schadsoftware.

Sperre einrichten

Schützen Sie Ihren Computer mit einem Passwort, PIN, Sperrmuster oder einer biometrischen Sperre vor unbefugtem Zugriff. Sollte Ihr Endgerät einmal in fremde Hände gelangen, sind sensible Daten so besser vor Missbrauch geschützt.

Aufpassen – Passwort

Komplexe Passwörter gewährleisten einen besseren Schutz

Verhalten Sie sich verantwortungsbewusst, indem Sie Ihren Computer mit einem sicheren Passwort schützen.

Tipps und Hinweise

Sichere Passwörter verwenden

Einfache Passwörter lassen sich mit Computerprogrammen innert Sekunden knacken. Ein sicheres Passwort beinhaltet die folgenden Merkmale:

– mindestens 10 Zeichen
– Ziffern, Gross- und Kleinbuchstaben sowie Sonderzeichen
– keine Tastaturfolgen wie zum Beispiel «asdfgh» oder «45678»
– kein Wort einer bekannten Sprache, d.h. das Passwort sollte keinen Sinn machen

Unterschiedliche Passwörter einsetzen

Verwenden Sie unterschiedliche Passwörter für die verschiedenen Geräte oder Programme. Benutzen Sie zum Beispiel für Ihr eBanking ein anderes Passwort als für Ihren E-Mail-Account.

Vorsicht bei Passwort-Diensten im Internet

Im Internet gibt es zahlreiche Webseiten und Hilfsprogramme, bei denen Sie prüfen können, wie gut Ihr Passwort

ist. Geben Sie hier nie Ihre echten Passwörter ein. Zur Erzeugung komplexer Passwörter empfiehlt sich die Nutzung eines Passwort-Generators. Achten Sie jedoch unbedingt darauf, den Generator von einer vertrauenswürdigen Quelle herunterzuladen (z.B. Empfehlungen von Vergleichsdiensten).

Regelmässig ändern

Ändern Sie Ihre Passwörter regelmässig und dabei umfassend. Ein Passwort, dass lediglich mit einem fortlaufenden Zähler erweitert wird, wird dadurch nicht sicherer. In einem Passwort-Manager können Sie alle Passwörter verschlüsselt abspeichern und müssen sich dadurch nur noch ein Passwort merken.

Nicht verraten

Teilen Sie Ihre Passwörter niemandem mit.

Zwei-Faktoren-Authentifizierung

Aktivieren Sie bei Online-Diensten die Zwei-Faktor-Authentifizierung und sorgen Sie damit für noch mehr Sicherheit. Wichtig: Die Zürcher Kantonalbank fragt nie – weder per E-Mail noch per Telefon – nach Ihrem Passwort oder nach der von Ihnen im eBanking verwendeten Transaktionsnummer (TAN). Sie verlangt auf diesem Weg auch nie einen Wechsel des Passwortes.

Ein sehr starkes Passwort generieren

Denken Sie sich zum Beispiel einen Satz aus, den Sie sich gut merken können, und setzen Sie die Anfangsbuchstaben zu einem Passwort zusammen: Ich fahre einen Golf 5, der auf meinem Parkplatz #105 steht! Passwort: IfeG5,damP#105s!

Aufpassen – Internet

Nicht alle Internetseiten sind echt

Diese unten abgebildete Webseite ist eine Fälschung! Sie ist nur eine von vielen nachgemachten Internetseiten. Die Angreifer versuchen, ganze Webseiten zu fälschen, um die Benutzer dazu zu verleiten, ihre persönlichen Daten einzugeben. Diese werden dann im Hintergrund ausgelesen. Häufig versuchen die Angreifer mit Hilfe von Links in E-Mails, die Benutzer auf die gefälschten Webseiten zu leiten.

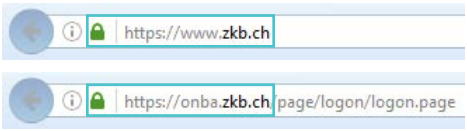
Tipps und Hinweise

So lassen sich imitierte Seiten erkennen

URL-Schreibweise beachten

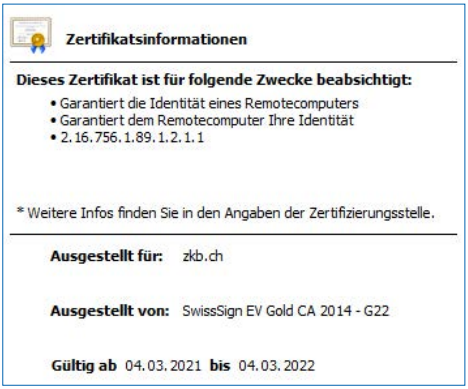
Achten Sie auf die korrekte Schreibweise, um sicherzustellen, dass Sie sich auf der richtigen Webseite befinden. Auch nur leichte Abänderungen können auf einen falschen Server leiten. Dabei sind vor allem die ersten Zeichen einer Webadresse entscheidend (Domain z. B. www.zkb.ch). Bei einer Fälschung werden häufig Buchstaben ausgetauscht oder ähnliche Bezeichnungen verwendet.

Achten Sie auf https und das Schloss-Symbol in der Adresszeile (wie in den Beispielen in der Abbildung). https bedeutet, dass die Daten verschlüsselt übertragen werden.



Zertifikate prüfen

Durch Klick auf das Schloss-Symbol können Sie das Sicherheitszertifikat einsehen.



Warnungen des Browsers beachten

Ihr Internetbrowser (zum Beispiel Internet Explorer, Edge, Firefox, Chrome, Safari) gibt je nach Einstellung und Version Hinweise auf unsichere Inhalte einer Webseite. Achten Sie auf diese Meldungen.

Inhalte hinterfragen

Hinterfragen Sie kritisch, ob die Inhalte, die Sie auf einer Webseite sehen, plausibel sind und dem entsprechen, was Sie erwarten. Bedenken Sie jedoch auch, dass Webseiten trügerisch genau nachgebaut sein können.

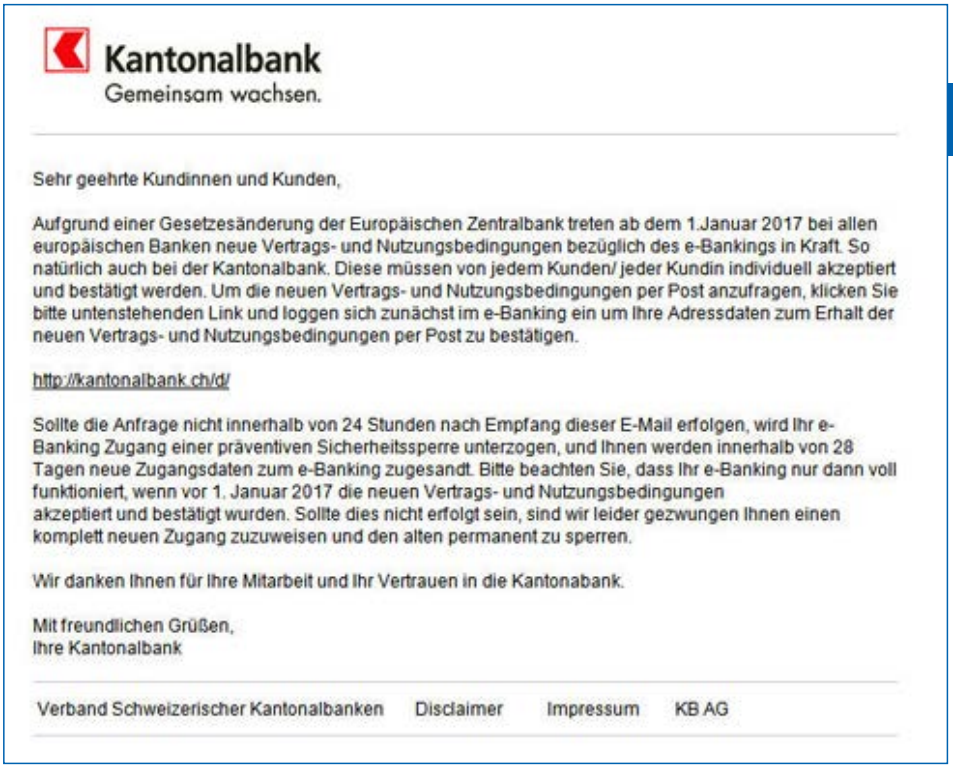
Fehlerhafte Funktionen sind verdächtig

Gefälschte Webseiten haben oft Fehler oder funktionieren nicht vollständig. Zum Beispiel wird lediglich das Login zum eBanking kopiert, um an persönliche Daten zu gelangen. Die übrigen Links und Funktionen können nicht angeklickt werden.

Aufpassen – E-Mail

E-Mails sind der direkte Weg der Angreifer auf Ihren Computer

Phishing-E-Mails zielen häufig darauf ab, die Kontrolle über Ihr eBanking zu übernehmen. Sie erhalten E-Mails von einem gefälschten Absender mit Anhängen oder Links, die Sie auf eine gefälschte Webseite führen. Diese Phishing-E-Mails sehen häufig authentisch aus. Die Angreifer verwenden Original-Logos und E-Mail-Adressen aus dem Internet. Lassen Sie sich nicht von echt aussehenden E-Mails täuschen. Der Link im E-Mail führt auf ein gefälschtes Webformular. Als Absender wird die Kantonalbank oder die Zürcher Kantonalbank vorgetäuscht.



Kantonalbank
Gemeinsam wachsen.

Sehr geehrte Kundinnen und Kunden,

Aufgrund einer Gesetzesänderung der Europäischen Zentralbank treten ab dem 1.Januar 2017 bei allen europäischen Banken neue Vertrags- und Nutzungsbedingungen bezüglich des e-Bankings in Kraft. So natürlich auch bei der Kantonalbank. Diese müssen von jedem Kunden/ jeder Kundin individuell akzeptiert und bestätigt werden. Um die neuen Vertrags- und Nutzungsbedingungen per Post anzufragen, klicken Sie bitte untenstehenden Link und loggen sich zunächst im e-Banking ein um Ihre Adressdaten zum Erhalt der neuen Vertrags- und Nutzungsbedingungen per Post zu bestätigen.

http://kantonalbank.ch/d/

Sollte die Anfrage nicht innerhalb von 24 Stunden nach Empfang dieser E-Mail erfolgen, wird Ihr e-Banking Zugang einer präventiven Sicherheitssperre unterzogen, und Ihnen werden innerhalb von 28 Tagen neue Zugangsdaten zum e-Banking zugesandt. Bitte beachten Sie, dass Ihr e-Banking nur dann voll funktioniert, wenn vor 1. Januar 2017 die neuen Vertrags- und Nutzungsbedingungen akzeptiert und bestätigt wurden. Sollte dies nicht erfolgt sein, sind wir leider gezwungen Ihnen einen komplett neuen Zugang zuzuweisen und den alten permanent zu sperren.

Wir danken Ihnen für Ihre Mitarbeit und Ihr Vertrauen in die Kantonabank.

Mit freundlichen Grüßen,
Ihre Kantonalbank

Verband Schweizerischer Kantonalbanken Disclaimer Impressum KB AG

Tipps und Hinweise

Verdächtige E-Mails löschen

Löschen Sie Phishing-E-Mails und klicken Sie auf keinen Fall auf den Anhang oder den Link.

Nicht installieren

Installieren Sie keine Software oder Apps, wenn Sie in einer E-Mail oder auf einer mutmasslich gefälschten eBanking-Login-Seite dazu aufgefordert werden – auch wenn es sich angeblich um eine Aufforderung der Zürcher Kantonalbank handelt.

So erkennen Sie Phishing-E-Mails

Inhalt

Bei E-Mails ist stets ein gesundes Misstrauen angebracht. Erwarten Sie das E-Mail wirklich und passt es in Ihren Kontext? Wenn Sie zum Beispiel eine Aufforderung erhalten, eine Rechnung zu bezahlen, Sie jedoch bei diesem Anbieter nichts bestellt haben, dann öffnen Sie auf keinen Fall die Rechnung im Anhang.

Links

Durch Klick auf einen Link in der E-Mail kann sich eine Schadsoftware installieren oder Sie werden auf eine gefälschte Webseite gelenkt. Prüfen Sie, wohin ein Link führt, indem Sie mit dem Mauszeiger darüberfahren. Denn dadurch wird der verknüpfte Link sichtbar. Klicken Sie nur, wenn Sie der dargestellten Adresse trauen.

Anhänge

Im Anhang des E-Mails kann Schadsoftware versteckt sein, die sich installiert, wenn Sie die Datei öffnen. Öffnen Sie keine Anhänge, wenn Sie dem Absender nicht vertrauen oder Ihnen etwas suspekt vorkommt.

Alte Office-Formate

Schadsoftware enthält immer einen Code. Vor allem bei alten Office-Formaten mit den Endungen .doc, .xls und.ppt ist nicht direkt ersichtlich, ob ein Code enthalten ist. Verwenden Sie deshalb die neuen und vom Hersteller empfohlenen Office-Formate .docx, .xlsx und .pptx.

Bilder herunterladen

Deaktivieren Sie in Ihrem E-Mail-Client die Funktion, Bilder in E-Mails automatisch herunterzuladen. Damit verhindern Sie, dass beim Öffnen der E-Mail-Inhalte automatisch geladen werden und allfälli-

ger Schadcode direkt ausgeführt wird.
Zeitdruck: Häufig versuchen Angreifer, die Empfänger des E-Mails zu schnellem Handeln zu drängen. Lassen Sie sich nicht hetzen und fragen Sie sich, ob Sie wirklich sofort reagieren müssen.

Versprechungen
Begegnen Sie allzu lukrativen Einkommensmöglichkeiten (hohe Anlagerenditen, Gewinnversprechen etc.) stets mit Skepsis.

Prävention

Kriminalität verunsichert – Prävention macht sicherer.

Die anspruchsvolle Aufgabe der Kantonspolizei Zürich besteht darin, bei grösstmöglicher individueller Freiheit ein hohes Mass an Sicherheit für alle zu gewährleisten. Die aktuellen Herausforderungen verlangen nach neuen präventiven Ansätzen in der Polizeiarbeit zur Bekämpfung der Kriminalität. Die Bevölkerung erwartet, dass die Polizei den Menschen nicht nur in Notsituationen hilft, sondern sie auch rechtzeitig auf Gefahren hinweist und sie davor schützt.

Diese Erwartung nehmen wir ernst. Wenn es uns gelingt, Gefahren vorausschauend zu erkennen und dagegen vorzugehen, um so Straftaten zu verhindern oder den Schaden zumindest in Grenzen zu halten, können wir am meisten bewirken. Diese wichtige Präventionsaufgabe packen wir im Wissen darum an, dass sie zu den schwierigsten der Polizeiarbeit gehört.

Die partnerschaftliche Vernetzung mit anderen Behörden und Institutionen sowie der gute Kontakt zur Bevölkerung sind uns wichtig. Die Polizei allein kann keine umfassende Sicherheit garantieren. Der Verbund mit vielen gesellschaftlichen Partnern ermöglicht uns, gemeinsam Wirkung zu erzielen und das Leben in unserem Kanton sicherer machen.

Sie selbst können durch richtiges Verhalten und mit geeigneten Massnahmen das Risiko massgeblich minimieren, Opfer eines Diebstahls, eines Betrugs oder einer Phishing-Attacke zu werden. Der Ratgeber der Zürcher Kantonalbank unterstützt Sie dabei.

Reinhard Brunner
Leiter Präventionsabteilung
Kantonspolizei Zürich

Kontakt
Kantonspolizei Zürich – Prävention
und Sicherheitsberatung
Telefon 044 295 98 39
praevention@kapo.zh.ch

kapo.zh.ch/internet/sicherheitsdirektion/
kapo/de/praevention.html

Hilfe bei Notfällen

Hier erhalten Sie in einem Notfall Hilfe.

Bankkarten
Kostenlose Sperrung der Bankkarte im eBanking oder eBanking mobile möglich
Sperrung von Maestro-, Konto- und Autosafekarten
Telefon 0844 843 823
Servicezeiten: 7×24 Stunden

Kreditkarten
Kostenlose Sperrung der Kredit- oder PrePaidkarte im eBanking via one App möglich
Sperrung von Kredit- und PrePaid-Karten
Telefon 058 958 83 83
Servicezeiten: 7×24 Stunden

eBanking
Sperrung eBanking und eBanking Mobile
Telefon 0844 840 140
Servicezeiten:
Montag – Freitag: 08.00 – 22.00 Uhr
Samstag / Sonntag: 09.00 – 18.00 Uhr

eBanking-Vertrag selbst sperren
Im Notfall können Sie Ihren eBanking-Vertrag selbst online sperren. Melden Sie sich dazu in Ihrem eBanking an und klicken Sie auf Einstellungen.

Sicherheit in der Zürcher Kantonalbank
Die Zürcher Kantonalbank schützt Informationen, Personen und Objekte mit umfassenden technischen und organisatorischen Massnahmen. Insgesamt sind über 100 Mitarbeitende mit der laufenden Beurteilung der Sicherheitsrisiken, der Umsetzung geeigneter Massnahmen und mit der permanenten Sicherheitsüberwachung betraut. Weitere Tipps und Hinweise finden Sie unter zkb.ch/sicherheit

Besondere Hinweise für Unternehmerinnen und Unternehmer
Das Merkblatt Informationssicherheit für KMU der Melde- und Analysestelle Informationssicherung MELANI richtet sich an Schweizer KMU und soll diese dabei unterstützen, die Informationssicherheit in ihrer Systemumgebung und ihrem Unternehmensnetzwerk zu erhöhen. Herausgeber: Eidgenössisches Finanzdepartement EFD, Informatiksteuerungsorgan Bund ISB. Das Merkblatt ist im Internet auf der Download-Seite unter vbs.admin.ch zu finden (MELANI-Informationssicherheit-KMU-d.pdf).

Rechtliche Hinweise

05/21 223586 In der Schweiz gedruckt auf 100% Recyclingpapier.