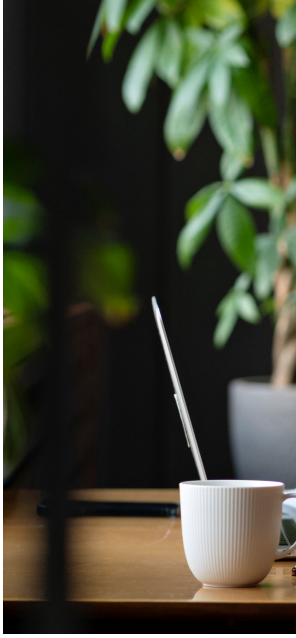
Online-Betrug kennt viele Facetten



Wo Vermögen ist, gibt es Diebe. Und weil sich das Leben und auch Finanzbelange immer mehr ins Internet verlagern, steigt die Zahl der Delikte. Wer aber aufmerksam sowie skeptisch ist und einige Vorkehrungen trifft, kann sich schützen.

Pflichtbewusst ist Max Mustermann. Darum reagiert er umgehend, als er ein E-Mail von seiner Bank erhält. Aufgrund einer Software-Aktualisierung sei es nötig, das Passwort zu ändern. Nichtsahnend klickt er auf den Link, gelangt auf die Anmeldeseite der Bank und ändert das Passwort. Was Herr Mustermann nicht weiss: Absender der E-Mail war nicht seine Bank. Sie stammte von Betrügern, ebenso die Webseite, auf der er seine E-Banking-Zugangsdaten eingegeben hat. Diese Daten – Vertragsnummer, das alte und das neue Passwort – sind nun in die Hände der Betrüger geraten.

Banken bauen Hürden für Betrüger ein

Nun ist es in der Regel so, dass Banken bei einem Login eine weitere Bestätigung anfordern – die sogenannte Zwei-Faktor-Authentifizierung. «Wir erschweren mit dieser technischen Hürde den Betrügern den Zugriff aufs Online-Banking und schützen damit unsere Kundinnen und Kunden», sagt Markus Zbinden, bei der TKB verantwortlich für Informationssicherheit. Wäre Herr Mustermann auf die gleiche Masche im Namen eines Online-Händlers hereingefallen, der zum Login keine Zwei-Faktor-Authentifizierung nutzt, hätten ohne Weiteres teure Elektronikgeräte oder Luxusartikel auf Rechnung von Herrn Mustermann bestellt werden können. Darum rät der Experte stets zu besonderer Vorsicht bei E-Mails mit der Aufforderung, Zugangsdaten bekannt zu geben oder zu ändern. «Keine seriöse Firma kontaktiert Kunden per E-Mail, Telefon oder SMS und fragt nach Login und Passwort», so der Experte.

Achtung vor Psycho-Fallen

Phishing – so heisst das Abgreifen von Daten mittels gefälschter Webseiten – ist eine der häufigsten Methoden von Internet-Kriminellen. Die Entwicklung von Kriminalität im Internet geht Schritt für Schritt einher mit der Entwicklung des digitalen Einkaufens und Bezahlens. Das Bundesamt für Cybersicherheit hat alleine im ersten Halbjahr 2024 6643 Phishing-Meldungen registriert, das waren fast 3000 mehr als im Vorjahreszeitraum. Die Betrüger gehen sehr professionell vor, und ihre Tricks werden immer raffinierter.

Kompaktseminar «Online-Sicherheit»

Wissenswertes rund um dass Thema Sicherheit im Internet vermitteln Expertinnen und Experten im Kompakt-Seminar «Online-Sicherheit». Das Seminar dauert 90 Minuten, ist kostenlos und richtet sich an alle Interessierten. Information und Anmeldung:

tkb.ch/seminar

Und sie üben Druck aus. Wer möchte schon den Zugriff auf das E-Banking verlieren? Kriminelle nutzen die Angst der Menschen vor Verlust schamlos aus. Hier setzt eine weitere Methode an: das sogenannte Social Engineering. Angreifende versuchen, mit psychologischen Tricks an vertrauliche Informationen zu gelangen. Hierbei setzen sie Druck auf oder täuschen Hilfsbedürftigkeit vor. Häufige Masche sind Telefonate von Softwarefirmen, die Zugriff auf das Gerät verlangen, um wichtige Updates zu machen. Installiert man dann wie aufgefordert eine Software, öffnet man den Tätern Tür und Tor zum eigenen Gerät.

Besser einmal mehr nachfragen

Gemäss Markus Zbinden ist immer dann Skepsis angebracht, wenn man ungefragt von angeblichen Dienstleistern kontaktiert wird. «Sobald der kleinste Zweifel aufkommt, hängt man am besten auf. Bei Bankangelegenheiten raten wir, die Beraterin, den Berater zu kontaktieren», sagt er. Überhaupt solle man digital – wie auch im «echten» Leben – nur Menschen vertrauen, deren Identität man verifizieren kann. Wichtig sei zudem, dass man es den Tätern auch im Falle eines gelungenen Angriffs schwierig oder unattraktiv mache. Ein Tipp des Experten: «Man sollte auf allen Konten im Online Banking Limiten für Höchstbeträge setzen. Damit kann man wenigstens den Schaden in Grenzen halten, falls doch einmal etwas passiert.»

Skepsis ist angebracht, wenn ein Unternehmen per Mail, Telefon oder SMS nach Login-Daten fragt.

Sicherheit im Web: zehn Tipps

- Unterschiedliche und lange Passwörter (mindestens zwölf Zeichen) nutzen, diese regelmässig ändern sowie Passwort-Manager-Apps einsetzen
- Niemals Passwörter weitergeben
- Die Zwei-Faktor-Authentifizierung nutzen
- Niemals verdächtige Links oder E-Mail-Anhänge öffnen, im Zweifel beim Absender nachfragen
- Prüfen, ob Links auch wirklich zum vermeintlichen Absender führen, Links manuell eingeben und nicht auf Links in E-Mails oder Google-Anzeigen klicken
- Bei verdächtigen Anrufen: auf keinen Fall unter Druck setzen lassen und auf die offizielle, zentrale Firmennummer zurückrufen
- Firewalls und Antivirensoftware nutzen und diese aktuell halten sowie regelmässig Back-ups durchführen
- Mit Benutzerkonten statt mit Administrator-Konten von den Geräten im Web surfen, denn: Schadsoftware erhält immer die gleichen Rechte wie der Benutzer, der sie sich einfängt
- Mehrere Konten nutzen und auf den «Bezahl»-Konten Limiten einrichten
- Informationen einholen – zum Beispiel bei «E-Banking, aber sicher», **www.ebas.ch**

Weitere Links
tkb.ch/ebanking-sicherheit
cybercrimepolice.ch
ncsc.ch

«Immer aufmerksam sein»

Daniel Meili, welche Art des Online-Betrugs stellt die Kantonspolizei am häufigsten fest?
Anders als vielleicht erwartet, sind es selten ausgeklügelte Hackerangriffe. Bei uns kommen in erster Linie Delikte zur Anzeige, die deutlich niederschwelliger sind. Klassiker im negativen Sinn sind etwa Betrügereien auf Online-Marktplätzen. Grosser Schaden entsteht aber auch durch Anlagebetrug, bei dem versprochene Traum-Investitionen immer in einem Totalverlust enden. Auch längst bekannte Maschen wie der spanische Lotteriegewinn oder Phishing-Nachrichten von angeblichen Behörden, Firmen oder Banken sterben nicht aus.

Wieso fallen immer noch viele Menschen darauf herein?
Weil es eben Menschen sind. Die Täter verstehen es sehr gut, unsere Emotionen anzusprechen und den vielzitierten gesunden Menschenverstand zu überlisten. Starke Emotionen und Gefühle wie Freude bei angeblichen Gewinnen, Superschnäppchen sowie Traumrenditen oder Angst wegen angeblichen Hackerangriffen lassen viele Menschen Dinge tun, die sie im Nachhinein bereuen. Die Opfer sind übrigens nicht wie oft zu hören dumm und senil, sondern meist Menschen wie du und ich, die einfach im falschen Moment auf dem falschen Fuss erwischt wurden.

Lohnt sich eine Anzeige bei der Polizei in jedem Fall?
Ja. Auch wenn je nach Delikt die Ermittlungschancen eher klein sind, helfen uns die Informationen, einen Betrug besser zu verstehen und möglicherweise national und international vernetzt doch eine Spur aufzunehmen.

Welches sind Ihre wichtigsten Tipps, um sich zu schützen?
Aufpassen, aufpassen und nochmals aufpassen. Wer nicht unüberlegt Links anklickt oder Anhänge öffnet und sich stattdessen Gedanken macht, ob das Superschnäppchen, die Traumrendite oder das furchterregende Mail wirklich echt sein könnten, macht schon sehr viel richtig. Natürlich ist es auch wichtig, Sicherheitsmechanismen wie die Zwei-Faktor-Authentifizierung oder sichere Passwörter konsequent anzuwenden und Firewall, Virenscanner und andere Software immer auf dem neuesten Stand zu halten.

Daniel Meili ist Fachspezialist Kriminalprävention bei der Kantonspolizei Thurgau.