

eBanking aber sicher!

Mobile Bezahlverfahren sicher nutzen

Hochschule Luzern – Informatik
Prof. Oliver Hirschi

SmartCard Forum
VIVAVIS Schweiz AG, Baden-Dättwil
14.05.2025

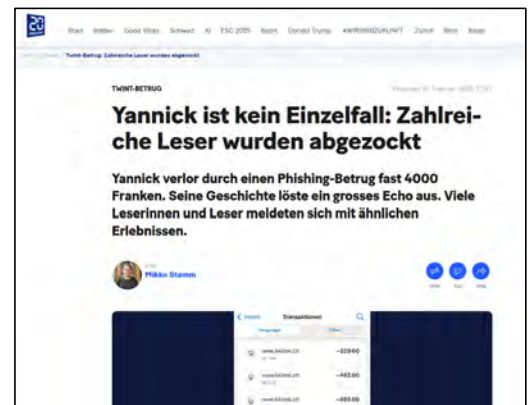
FH Zentralschweiz



«eBanking – aber sicher!» – Mobile Bezahlverfahren sicher nutzen

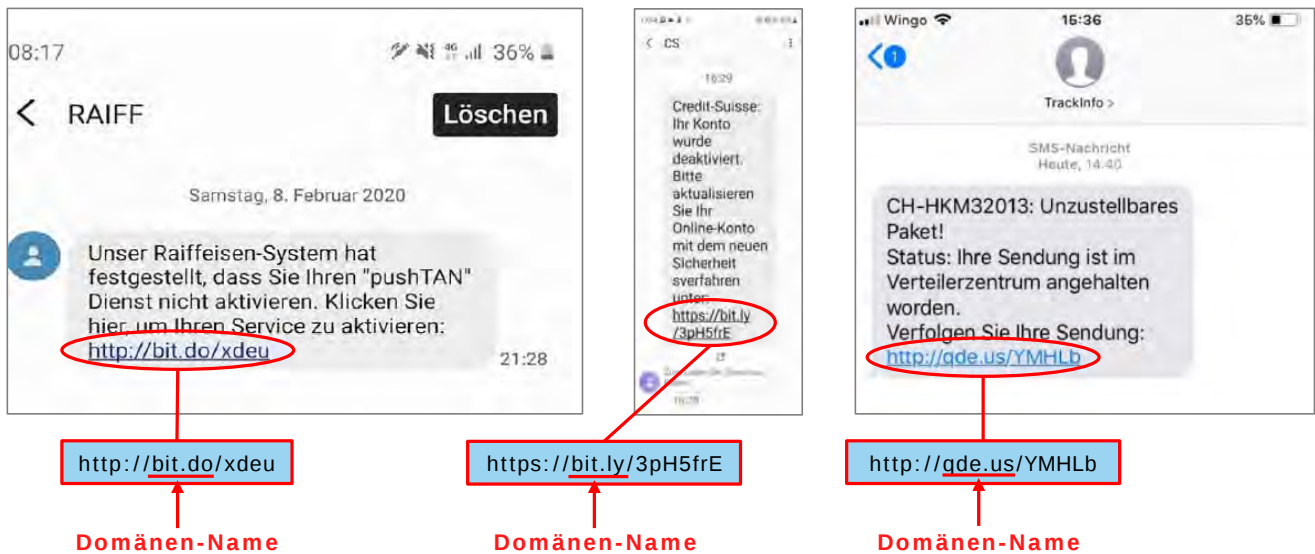
Aktuelle Top-Bedrohung: TWINT-Marketplace-Fraud

- Betrüger interessieren sich für ein Produkt.
- Inserent erhält (via WhatsApp) einen Link oder QR-Code, um das Geld zu erhalten.
- Der Link führt auf eine täuschend echt aussehende Phishing-Webseite von TWINT oder dem E-Banking mit ähnlich lautender URL.

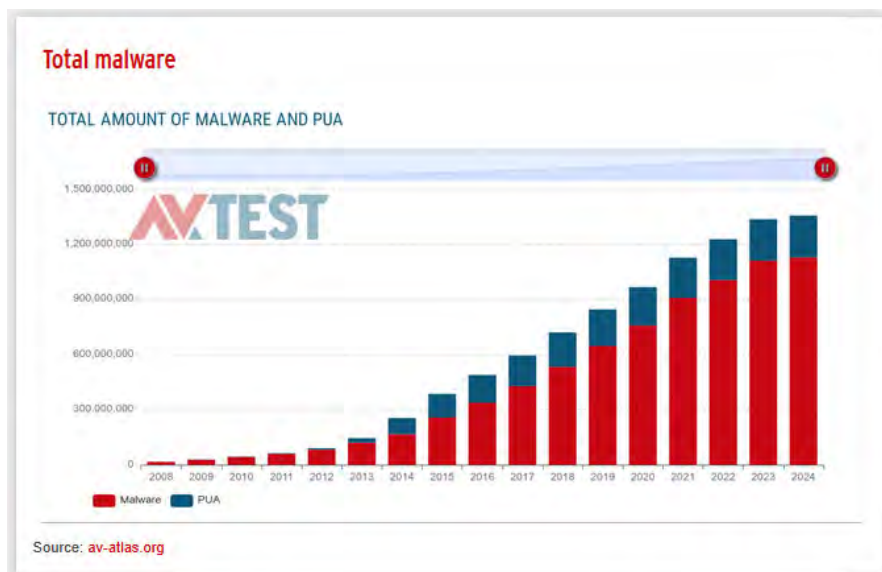


→ Geben Sie nie Ihre E-Banking-Zugangsdaten, Ihren TWINT-Code oder Ihre Debit- oder Kreditkartendaten auf dieser Phishing-Website ein! Dadurch erhalten die Betrüger Zugang zu Ihrem E-Banking oder TWINT.

Aktuelle Bedrohungen: Smishing Gefälschte SMS / Kurznachrichten



Aktuelle Bedrohungen: Android-Malware



«Grundschutz» für Mobilgeräte

- Mobilgerät schützen («**5 Schritte für Ihre digitale Sicherheit**»)
 - Backup, Virenschutz, Updates, Zugriffsschutz, Aufpassen
- Apps nur aus dem **offiziellen Store** installieren
- Nur wirklich **benötigte Apps** installieren
- **Zugriffsrechte** aller Apps aufs Nötigste beschränken
- Nur mit **vertrauenswürdigen Netzwerken** verbinden
- Bei Verlust Gerät sofort sperren, und vor Verkauf oder Entsorgung korrekt zurücksetzen

→ www.ebas.ch/mobilebanking

Was ist Mobile Payment?

- Früher ...
 - ... bezahlte man mit Bargeld.
- Heute ...
 - ... bezahlt man mit **mobilen Geräten**.
- Unter Mobile Payment versteht man das **Bezahlen mit mobilen Geräten (Smartphone, Tablet, Smartwatch etc.)**.
- Arten von Mobile Payment:
 - **Mobile Payment = Bezahlmethode** in Läden, beim Online-Einkauf, bei Automaten etc.
 - **P2P Payment = Geldüberweisung** (Peer-to-Peer) von einer Person auf eine andere Person.



Voraussetzungen für Mobile Payment Bezahlmethode

- Voraussetzungen für den **Zahler** (je nach Anbieter):
 - Smartphone, Tablet, Smartwatch etc. mit NFC-Unterstützung oder Kamera
 - Hinterlegte Kredit- oder Debitkarte
 - Geladenes Guthaben auf der App
 - Verbundenes Bankkonto mit der App
- Voraussetzungen für den **Händler (Zahlungsempfänger)**:
 - Terminal mit ...
 - NFC-Unterstützung
 - QR-Code-Anzeige

NFC (Near Field Communication)

- Bezahlen via **NFC** (Near Field Communication).
 - Datenübertragung via Nahfunktechnik über einen Chip.
- Ein internationaler **Übertragungsstandard** zum drahtlosen Austausch von Daten über kurze Distanzen.
 - **10 - 20 Zentimeter**
- Basierend auf der RFID-Technik (Radio-Frequency Identification).
- Inzwischen in fast allen **mobilen Geräten** ab Werk integriert.
- Nützliche Funktionen:
 - Bezahlen per Smartphone
 - EC-Karten und Kreditkarten mit NFC-Chip
 - Tickets für Konzerte und Veranstaltungen
 - Datenaustausch zwischen mobilen Geräten



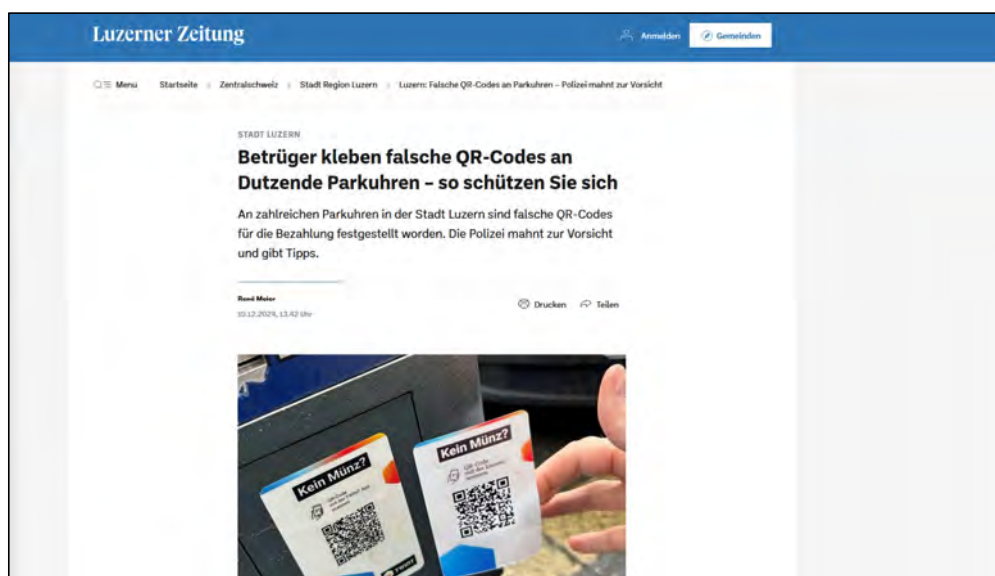
QR-Code (Quick Response Code)

- Bezahlen via **QR-Code** (Quick Response Code).
 - Datenübertragung durch einscannen des QR-Codes.
- Ein **zweidimensionaler Code**.
- Bestehend aus einer **quadratischen Matrix** aus schwarzen und weissen Quadraten, die die kodierte Daten binär darstellen.
- Eine **spezielle Markierung** in drei der vier Ecken des Quadrats gibt die Orientierung vor.
- Die Daten im QR-Code sind durch einen **fehlerkorrigierenden Code** erweitert. Dadurch wird der Verlust von bis zu 30 % des Codes toleriert, d. h., er kann auch dann noch dekodiert werden.
- Nützliche Funktionen:
 - Bezahlen per Smartphone
 - Führen zu Inhalten



QR-Code von «eBanking – aber sicher!»
führt zu www.ebas.ch

QR-Code: Risiken



QR-Code: Wichtige Schutzmassnahmen

- Nutzen Sie ausschliesslich QR-Code Scanner, welche Ihnen den Inhalt des Codes erst anzeigen, und ihn nicht sofort weiterverarbeiten.
- Prüfen Sie nach dem Scannen eines QR-Codes immer die **Link-Destination (Domänen-Name)** oder **Zahlungsinformation**, bevor Sie die Zielseite öffnen oder die Transaktion ausführen.
- Lassen Sie sich von niemandem zu Zahlungen mittels QR-Codes überreden.
- Nutzen Sie QR-Codes ausschliesslich in Situationen, in welchen Sie deren Verwendung für normal bzw. unbedenklich halten.
- Wenn Sie befürchten, dass Sie betrogen wurden, alarmieren Sie umgehend Ihr Finanzinstitut und ändern Sie sofort Ihre Zugangsdaten.

Anbieter von Mobile Payment

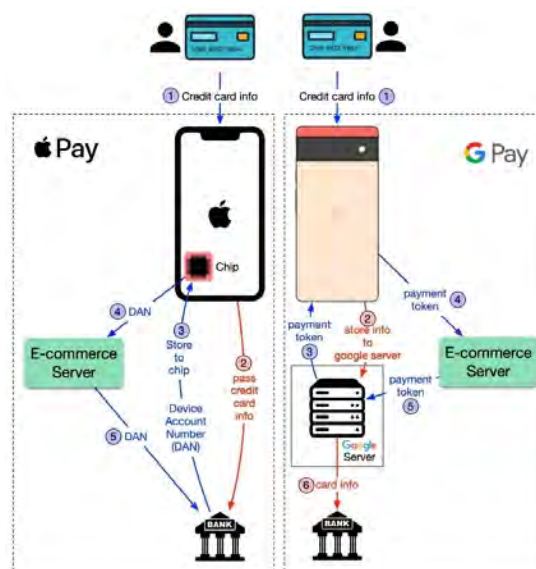
- Lösungen von Schweizer Unternehmen:
 - Twint – Bezahlmethode und Geldüberweisung
 - ...
- Lösungen von internationalen Unternehmen:
 - Amazon Pay – Reine Bezahlmethode
 - Apple Pay – Reine Bezahlmethode
 - Google Pay – Reine Bezahlmethode
 - PayPal – Bezahlmethode und Geldüberweisung
 - Samsung Pay – Reine Bezahlmethode
 - ...



Mobile Payment: Risiken

- **Physischer Verlust oder Diebstahl des Gerätes**
 - Missbräuchliche Zahlungen
 - **Identitätsdiebstahl**
 - Betrug auch möglich, wenn Sie noch im Besitz Ihres mobilen Gerätes sind!
 - Durch Malware, Phishing oder Social Engineering Diebstahl Ihrer Zugangs- oder Bezahl Daten.
 - Missbräuchliche Zahlungen
 - **Verletzung der Privatsphäre (Datenschutz)**
 - Der Anbieter der App soll nicht erfahren, was Sie wo gekauft haben!
 - Der Händler soll nicht erfahren, wie hoch Ihr Kontostand ist!
- Lässt sich nur schwer überprüfen ...

Umgang Vertrauliche Karteninformationen Apple Pay vs. Google Pay



Mobile Payment: Wichtige Schutzmassnahmen

- **Schützen Sie den Zugang zur Mobile Payment App.**
 - Aktivieren Sie die Sicherheitseinstellungen der App.
 - Richten Sie die automatische Sperre mittels Code, Passwort, **Fingerabdruck** oder **Gesichtserkennung** ein.
- **Geben Sie nur die wirklich notwendigen Daten der Mobile Payment App preis.**
 - Die Gefahr des Datenmissbrauchs entsteht durch eine mögliche Verknüpfung von Zahlungs- und Einkaufsdaten mit Nutzungs- und Standortdaten zu aussagekräftigen Nutzerprofilen.

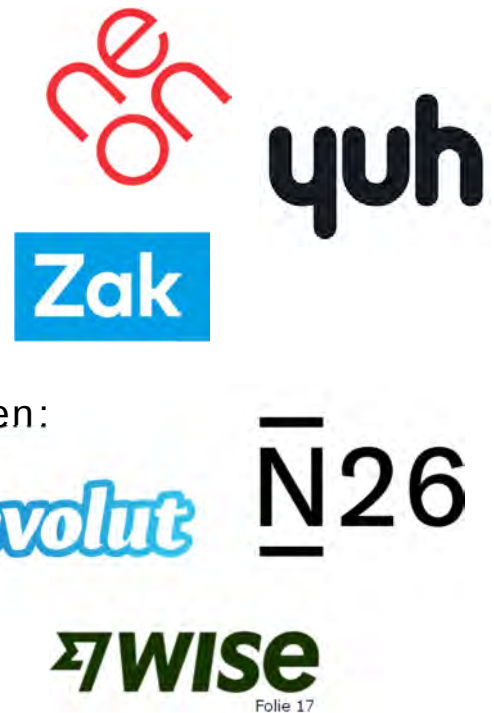
Internetbanken

- Auch als **Online-Banken**, **Smartphone-Banken** oder **Direktbanken** bezeichnet.
- Merkmale:
 - Internetbanken bieten ihre Produkte ausschliesslich übers Internet an.
 - Internetbanken unterhalten keine Filialen oder Callcenter.
 - Kunden kommunizieren mit der Internetbank hauptsächlich über Chat, E-Mail oder Telefon.
 - Internetbanken sind durch Kosteneinsparung «günstig».



Internetbanken: Anbieter

- Lösungen von Schweizer Unternehmen:
 - Neon
 - Yuh
 - Zak
 - ...
- Lösungen von internationalen Unternehmen:
 - N26
 - Revolut
 - Wise
 - ...

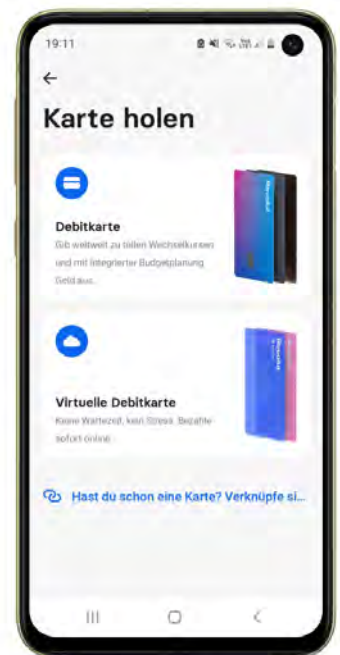


Internetbanken: Wichtige Schutzmassnahmen

- Seien Sie sich der **Problematik von Auslandsbanken** bewusst – erwarten Sie beispielsweise nicht die gleiche Qualität und den gleichen Support wie bei herkömmlichen Finanzinstituten.
- Verwenden Sie Internetbanken **nicht als einzige Bank, sondern nur als zusätzliches Konto**, mit welchem Sie beispielsweise in den Ferien günstig bezahlen können.
- Verlassen Sie sich in den Ferien **nicht nur auf eine Zahlungsmöglichkeit**, sondern halten Sie stets eine zweite Variante bereit – dies gilt im Übrigen generell und nicht nur für Internetbanken.
- Laden Sie auf das Konto der Internetbank **nur so viel Geld, wie in absehbarer Zeit benötigt wird**.

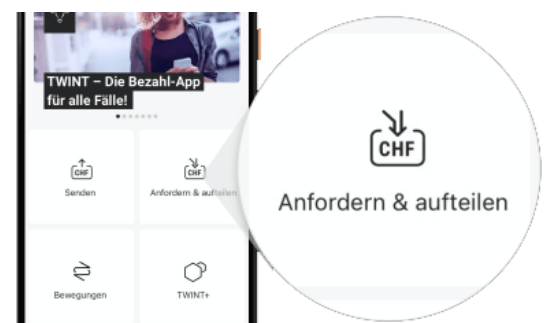
Revolut: Virtuelle Einwegkarte

- Rein **digitale Kreditkarte** für den **einmaligen Gebrauch**
- Vorteile:
 - Wird bei Bedarf kostenlos und unmittelbar erstellt
 - Händler können nur eine einmalige Belastung vornehmen
 - Erhalt einer Rückerstattung möglich



Tipp für Peer-to-Peer-Zahlungen (P2P-Zahlungen)

- Übertragen Sie mit Mobile Payment und Internetbanken Apps grössere Geldbeträge **nicht über die Senden-Funktion**, sondern immer nur über die **Anfordern-Funktion**.
 - So kommt nämlich bei einem Tippfehler etc. nicht das Geld, sondern nur die Anforderung beim falschen Empfänger an!



Newsletter von «eBanking – aber sicher!»

- Abonnieren Sie unseren Newsletter und verpassen Sie keine wichtigen Informationen!

→ www.ebas.ch/newsletter



Prof. Oliver Hirschi – © Hochschule Luzern – Informatik

Herzlichen Dank!

Fragen & Antworten

