HSLU Hochschule Luzern

eBanking aber sicher!

Aktuelle Cyberrisiken und Schutzmassnahmen

Hochschule Luzern – Informatik
Prof. Oliver Hirschi

18. April 2024

FH Zentralschweiz

HSLU Hochschule Luzern

Agenda

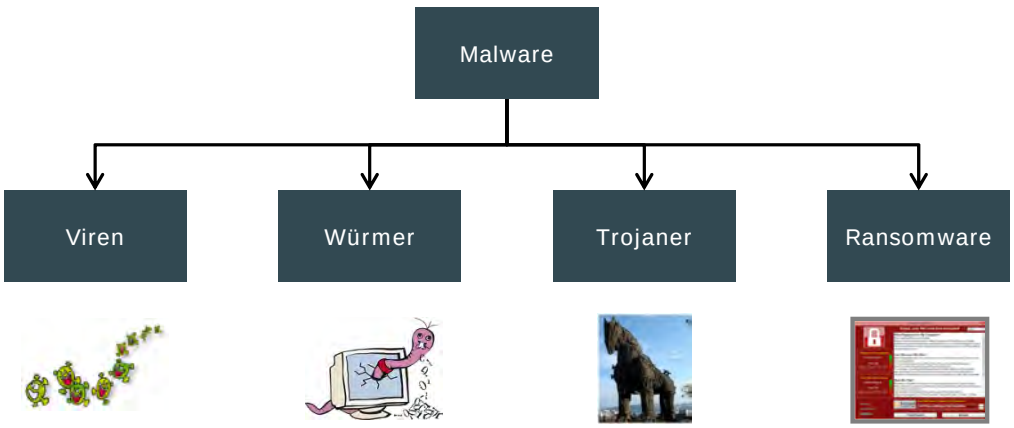
- **Bedrohungen**
  - Malware, Ransomware, Drive-by-Infektion
  - Social Engineering, Phishing
- **Massnahmen für mehr Informationssicherheit**
  - Grundschutz: «5 Schritte für Ihre digitale Sicherheit»
  - Passwortqualität
  - Umgang mit Social Media
  - Sicheres E-Banking

BEDROHUNGEN

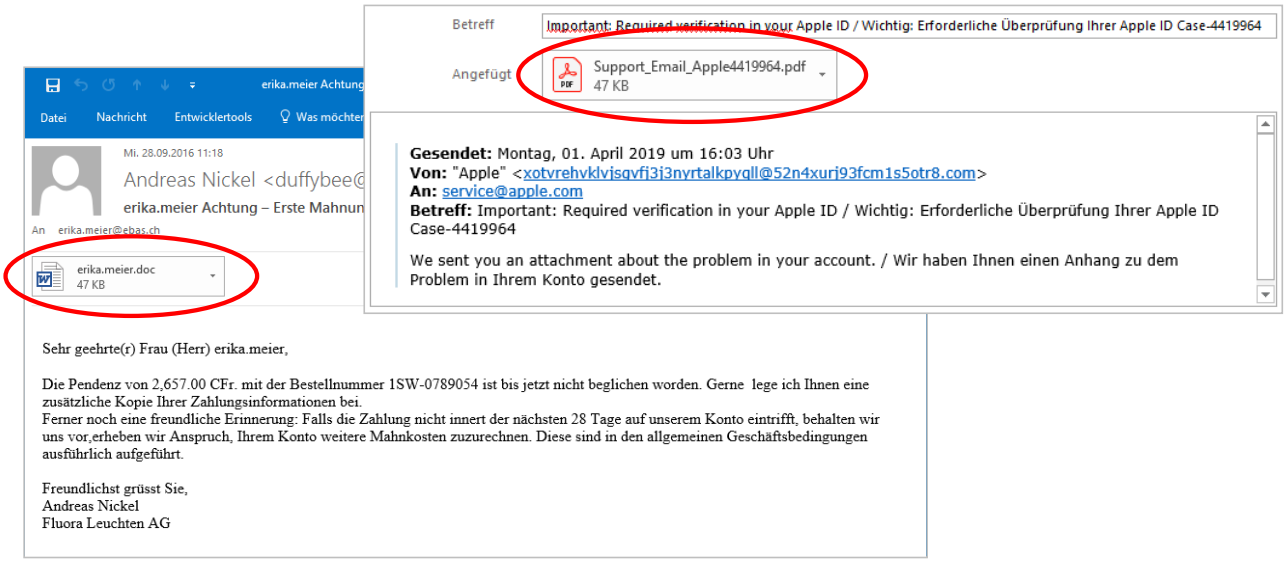
HSLU Hochschule Luzern

Malware

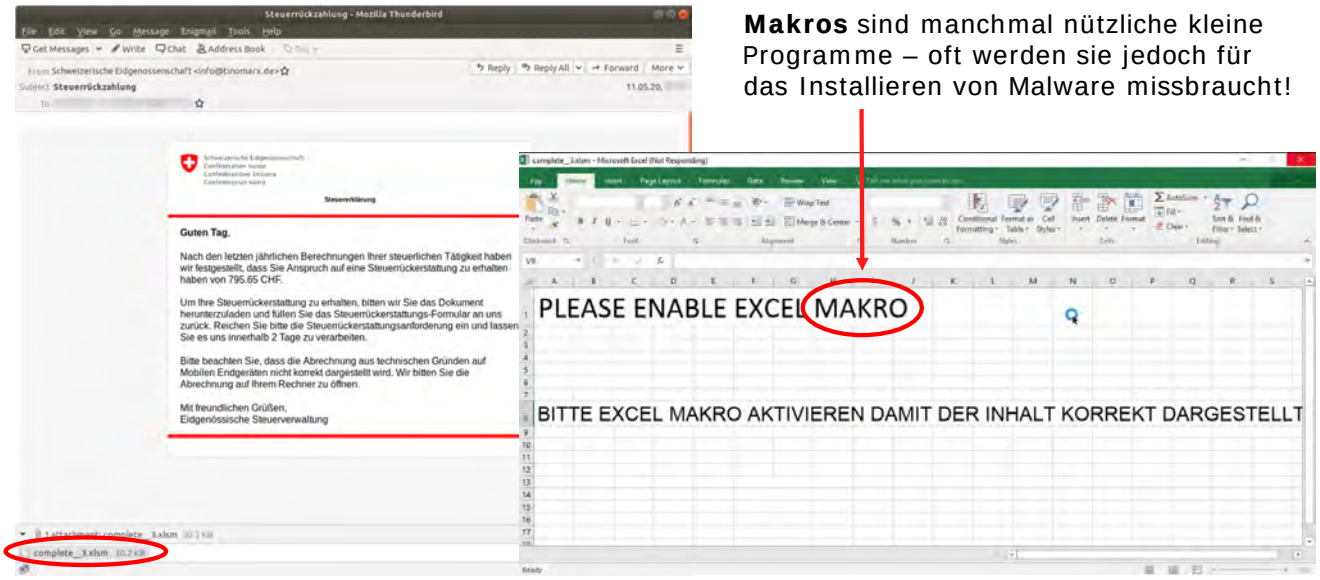
- Computerprogramme mit schädlichen Funktionen



Wie erfolgt eine Infektion?
Gefährliche E-Mail-Anhänge: Word, PDF …



Wie erfolgt eine Infektion?
Gefährliche E-Mail-Anhänge: Excel …



Makros sind manchmal nützliche kleine Programme – oft werden sie jedoch für das Installieren von Malware missbraucht!

Wie erfolgt eine Infektion?
Drive-by-Download

- Infizierung des Computers durch Malware lediglich durch das Besuchen einer Webseite
- Webseite von Angreifer modifiziert
- Über aktive Elemente der Webseite (Skripts) wird Malware auf dem Benutzer-PC installiert
- Auch «Offizielle» von bekannten Organisationen sind betroffen

Quelle: www.20min.ch

E-Banking-Malware «Gozi» via «20 Minuten» verbreitet (April 2016)

Social Engineering

- Eine verbreitete Methode zum **Ausspionieren von vertraulichen Informationen**
- Angriffsziel: Immer der **Mensch**
- Beispiele:
  - Eine Person gibt sich als **Techniker** aus (z. B. einer Telefongesellschaft, eines Elektrizitätswerkes etc.) und versucht so Zugang in Ihr Haus zu erlangen.
  - Sie erhalten eine **E-Mail** oder **Kurznachricht**, welche Sie auffordert einen Link aufzurufen und ein Login zu tätigen oder persönliche Informationen preis zu geben.
  - Eine Person gibt sich als **Polizist** oder **Bankangestellter** aus und ruft Sie per Telefon an und will Ihnen gewisse Fragen stellen (z. B. zum Einkommen, zu Sicherheitsmassnahmen am Computer etc.).
  - Ein Angreifer fälscht den **Absender** einer E-Mail oder Kurznachricht und gibt sich so als bekannte Person aus (möglicherweise enthält der Anhang eine Malware).

Phishing

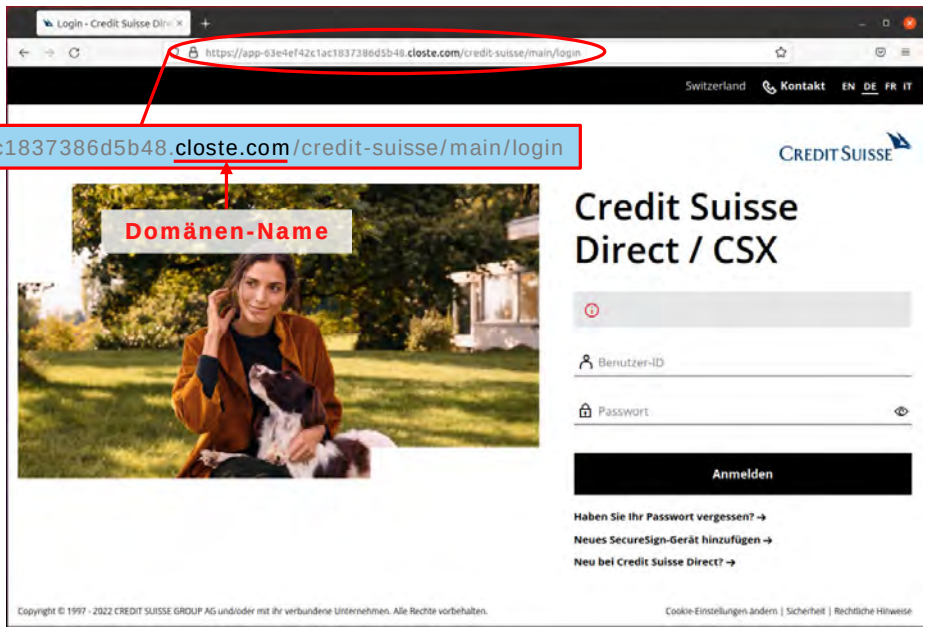
- Phishing: Kunstwort aus «password» und «fishing»
- Bedeutung: Nach Passwörtern fischen
- Ziel: **Vertrauliche Informationen**, wie z. B. Zugangsdaten zum E-Banking
- Begehrte Angriffsziele:
  - Finanzinstitute
  - Bezahldienstleister (PayPal etc.)
  - etc.
- Alternativ oder zusätzlich werden solchen Nachrichten oft auch Anhänge beigefügt, welche eine **Malware** enthalten!

Phishing: Gefälschtes E-Mail

Phishing: Gefälschte Webseite

https://app-63e4ef42c1ac1837386d5b48.closte.com/credit-suisse/main/login

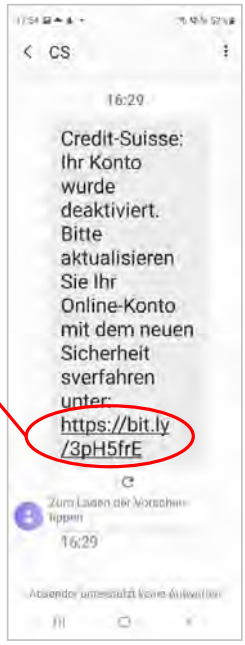
Domänen-Name

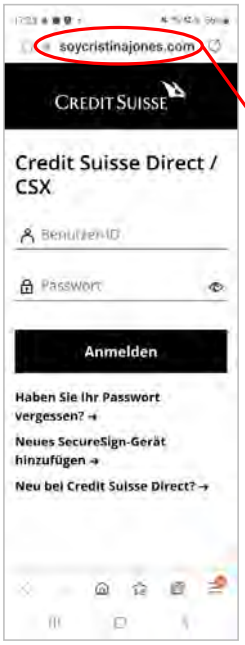


Smishing: Gefälschtes SMS und gefälschte Webseite

https://bit.ly/3pH5frE

Domänen-Name





soyccristinajones.com

Domänen-Name

Phishing-Varianten

- Klassisches Phishing → Via E-Mail
- Smishing (SMS-Phishing) → Via Kurznachrichtendienst (SMS, WhatsApp etc.)
- Vishing (Voice-Phishing) → Via Telefon
- QR-Phishing → Via QR-Code (Quick Response-Code)
- Spear Phishing → Via Social Engineering-Techniken

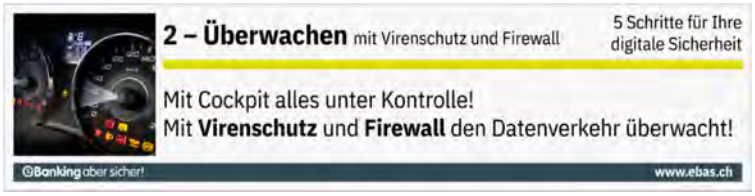
→ **Bereits das Anklicken eines Links in einer Nachricht genügt!**
(Drive-by-Download)

- **Phishing-Test**
  - Können Sie Phishing-Mails von legitimen E-Mails unterscheiden?

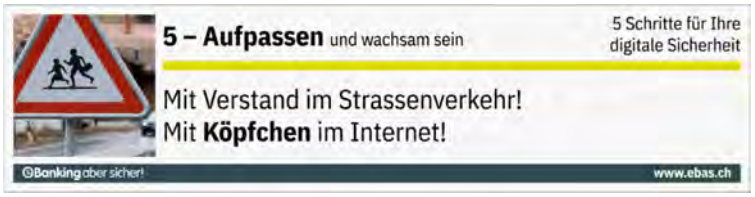
  → **www.ebas.ch/phishingtest**

MASSNAHMEN FÜR MEHR INFORMATIONSSICHERHEIT

Zusammenfassung I



Zusammenfassung II



www.ebas.ch

Was ist ein starkes Passwort?

- **Einfaches, 6-stelliges Passwort**
  36^6 = 2’176’782’336 Varianten

  → **Im Minutenbereich geknackt!**

- **Komplexes, 12-stelliges Passwort**
  95^{12} = 540’360’087’662’636’962’890’625 Varianten

  → **Tausende Jahre!**

Starke Passwörter

- Benutzername und Passwort sind nach wie vor die gängigsten und meistverwendeten Schlüssel zur elektronischen Identität!
- 6 Regeln zum starken Passwort – verwenden Sie:
  - **Mindestens 12 Zeichen**
  - **Ziffern, Gross- und Kleinbuchstaben sowie Sonderzeichen**
  - **Keine Tastaturfolgen wie z. B. «asdfgh» oder «45678»**
  - **Kein Wort einer bekannten Sprache – d. h. das Passwort sollte keinen Sinn machen**
  - **Überall ein anderes Passwort**
  - **Speichern Sie Ihr Passwort nicht unverschlüsselt ab**

Tipps zum starken Passwort

- Merken Sie sich Ihr Passwort mithilfe eines **Passwort-Satzes**
  - «**M**eine **T**ochter **T**amara **M**eier **h**at **a**m **19. J**anuar **G**eburtstag**!**»
  - «**MTTMha19.JG!**»
- Verwenden Sie einen **Passwort-Tresor**
  - KeePass (www.keepass.info)
  - Password Safe (www.passwordsafe.de)
  - SecureSafe (www.securesafe.com)
  - 1Password (www.1password.com)
  - Schlüsselbund
- Passwort **nie** im Browser abspeichern!

Schutz vor Social Engineering

- Geben Sie **möglichst wenig persönliche Informationen** über sich preis. Insbesondere auf **Sozialen Netzwerken** wie z. B. Facebook sollten Sie mit Informationen sehr sparsam umgehen.
- Geben Sie **Passwörter oder TAN-Codes** grundsätzlich **nie einer anderen Person bekannt** – auch einem Supportmitarbeitenden oder der Polizei nicht. Ein Passwort gehört Ihnen und nur Ihnen!
- Seien Sie bei Anfragen per E-Mail, Kurznachricht oder Telefon misstrauisch. Auch E-Mails und Kurznachrichten von **bekannten Absendern** und Anrufe von **bekannten Telefonnummern** können gefälscht sein!

→ **www.ebas.ch/socialengineering**

Social Media – WhatsApp, Instagram, YouTube etc.

- Zurückhaltung beim Veröffentlichen von Informationen
- **Zugriff** auf die veröffentlichten Informationen **einschränken** (Privatsphäre-Einstellungen)
- **Personen** als Freunde/Follower annehmen, die Sie **auch sonst kennen**
- Ein **«gesundes Mass an Misstrauen»** haben bei Nachrichten von unbekannten Personen
- Keine **Links aus unbekannten Quellen** aufrufen und Dokumente, Bilder, Videos etc. vor dem Öffnen prüfen.

«eBanking – aber sicher!» – Grundkurs

Social Media – WhatsApp, Instagram, YouTube etc.

- Soziale Medien bieten viele **Konfigurationsmöglichkeiten**. Unsere **Checklisten** unterstützen Sie bei der sicheren Konfiguration.
- Sie finden **die Checklisten** unter nachfolgenden Links:
  - Facebook: https://www.ebas.ch/facebooksettings
  - Twitter: https://www.ebas.ch/twittersettings
  - LinkedIn: https://www.ebas.ch/linkedinsettings
  - Instagram: https://www.ebas.ch/instagramsettings

Sicheres E-Banking – Beachten Sie …

beim Anmelden | während des E-Bankings | beim Abmelden

- **Sichere Navigation zum Finanzinstitut**
  - Tippen Sie die Adresse zum E-Banking Ihres Finanzinstituts immer **manuell** in der Adresszeile Ihres Browsers ein. Verwenden Sie niemals einen Link, welcher Ihnen z. B. per E-Mail zugestellt wurde! Ausserdem empfehlen wir, E-Banking nur von einem bekannten und sicheren Computer aus zu benutzen (d. h. nicht in Internet Cafés etc.).
- **Überprüfen der «sicheren» Verbindung**
  - Achten Sie darauf, dass Sie über eine «sichere» Verbindung (**Schlosssymbol**, **Name des Finanzinstituts** und **korrekter Domain-Name** in der Adresszeile) mit Ihrem Finanzinstitut verbunden sind und überprüfen Sie das Zertifikat.

Sicheres E-Banking – Beachten Sie …

beim Anmelden | während des E-Bankings | beim Abmelden

- **Systemunterbruch, ungewöhnliche Fehlermeldungen**
  - Kommt es beim E-Banking während der Internetsitzung zu einem Systemunterbruch (z. B. plötzlich auftretender weisser Bildschirm) oder treten v. a. während dem Login ungewöhnliche Fehlermeldungen auf (z. B. «Das System ist derzeit überlastet. Bitte haben Sie etwas Geduld und probieren Sie es später noch einmal!»), beenden Sie bitte sofort die Verbindung und benachrichtigen Sie die Spezialisten Ihres Finanzinstitutes.
- **Mobile Banking**
  - Achten Sie unterwegs darauf, dass Sie Ihre Anmeldeinformationen verdeckt eingeben, und dass Ihnen dabei **niemand über die Schulter blickt**.

Sicheres E-Banking – Beachten Sie …

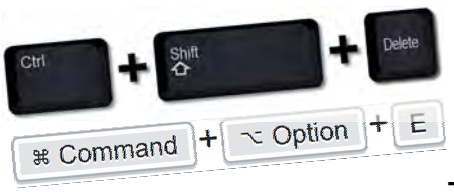
beim **Anmelden** | **während des E-Bankings** | beim **Abmelden**

- Achten Sie auf **ungewöhnliche Vorkommnisse** während einer aktiven E-Banking-Sitzung und melden Sie solche dem Finanzinstitut.
- Lesen Sie alle **Bestätigungsmeldungen** aufmerksam, bevor Sie diese quittieren.
- Lassen Sie offene E-Banking-Sitzungen **nie unbeaufsichtigt**.

Sicheres E-Banking – Beachten Sie …

beim **Anmelden** | **während des E-Bankings** | beim **Abmelden**

- **Korrektes Beenden der E-Banking Sitzung**
  - Beenden Sie die E-Banking-Sitzung korrekt über die dafür vorgesehene Funktion (meist mit «Abmelden», «Logout» oder «Beenden» gekennzeichnet).
- **Browserverlauf löschen**
  - Löschen Sie nach jeder Abmeldung der E-Banking-Sitzung den Browserverlauf (Cookies).

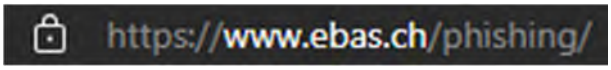


→ www.ebas.ch/infosheets

Überprüfung der sicheren Verbindung

- Es muss sichergestellt sein, dass eine sichere Verbindung (TLS-Verbindung) zum Finanzinstitut aufgebaut wurde.
- Die Merkmale, welche eine **sichere Verbindung** zur richtigen Webseite auszeichnen, sind:
  - Browser zeigt **Schloss-Symbol** in der Adresszeile
  - Browser zeigt den richtigen **Namen des Finanzinstituts**
    - Wird entweder neben dem Schloss oder nach einem Klick auf das Schloss unter «Ausgestellt für:» angezeigt
  - Browser zeigt den **richtigen Domänen-Namen** in der Adresszeile

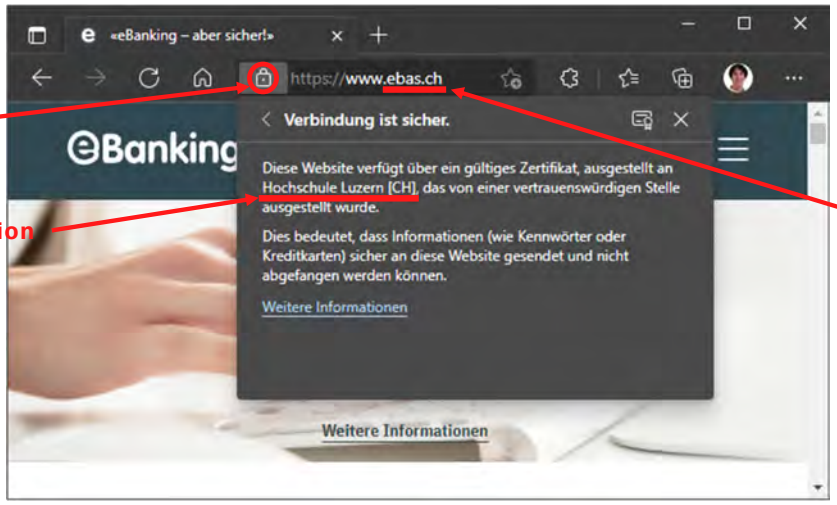
Wie finden Sie den richtigen Domänen-Namen?

- Eine Internetadresse ist wie folgt aufgebaut: 

  1. Übertragungsprotokoll: «**https://**»
  2. Vollständiger **Domänen-Name**
  3. Verzeichnispfad beginnend mit dem ersten Schrägstrich «**/**» (optional)
  4. Parameter beginnend mit dem ersten Fragezeichen «**?**» (optional)
- Der vollständige Domänen-Name einer Internetadresse befindet sich zwischen dem Übertragungsprotokoll und dem ersten Schrägstrich «**/**» oder Fragezeichen «**?**»
- Massgebend sind die **letzten zwei Begriffe** (getrennt durch einen Punkt «**.**») vor dem ersten Schrägstrich «**/**» oder Fragezeichen «**?**» → **ebas.ch**

→ **www.ebas.ch/internetaddress**

Microsoft Edge 121 und neuer



HINWEISE

Newsletter von «eBanking – aber sicher!»

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

→ www.ebas.ch/newsletter

«eBanking – aber sicher!» – Grundkurs

Kursübersicht von «eBanking – aber sicher!»

- **Grundkurs**
  - Lernen Sie die aktuellen Bedrohungen im Internet kennen und wie Sie sich mit einfachen Massnahmen davor schützen und E-Banking sicher anwenden.
- **Kurs Mobile Banking / Payment**
  - Lernen Sie Mobile Banking und Mobile Payment kennen und wie Sie solche Apps sicher nutzen.
- **Kurs Kryptowährungen**
  - Lernen Sie die wichtigsten Kryptowährungen und die zugrundeliegende Technologie Blockchain kennen und was betreffend Sicherheit zu beachten ist.
- **Kurs für unter 30-jährige**
  - Lerne dein Smartphone sicher zu verwenden. Neben Basics zeigen wir dir, was bzgl. Social Media, Clouds, Mobile Banking und Mobile Payment wichtig ist.

→ www.ebas.ch/course

HSLU Hochschule Luzern

Herzlichen Dank!

Fragen & Antworten

Hochschule Luzern – Informatik
Prof. Oliver Hirschi

FH Zentralschweiz