Sicherheit im Internet

lifebeats

lyondellbasell

Wie sicher ist Ihre Online-Identität?

*Einige der hier vorgestellten Software-Anwendungen und Lösungen dienen ausschließlich der **Information** und können nur **auf Ihrem privaten Computer** (nicht auf LyondellBasell-Geräten) **auf eigenes Risiko** installiert werden. LyondellBasell oder ihre verbundenen Unternehmen übernehmen keine Haftung für logische oder physische Schäden an Ihrem Gerät oder Ihren Daten.*

Ihre Online-Identität ist Ihr Ausweis für den Zugang zu Millionen von Online-Diensten, die im Netz angeboten werden - von E-Mails bis zu Unternehmensanwendungen, Onlineshops und auch Handys.

Haben Sie je über die Gefahr nachgedacht, dass Sie Ihre Online-Identität verlieren oder enthüllen könnten?

Gefahren bei E-Mails

- Ein einziges E-Mail-Konto für all Ihre Online-Aktivitäten
  - erschwert das Navigieren zwischen legitimen und “sonstigen” Mails, die Sie erhalten
  - ist ein „Single Point of Failure“ (zentrale Schwachstelle) – Wenn auf dieses E-Mail-Konto kein Zugriff mehr möglich ist, gibt es meistens keinen “Plan B”
  - bietet unzureichende Möglichkeiten zum Schutz gegen das aktuell häufig vorkommende E-Mail Phishing

Sie brauchen nur Ihre E-Mail-Adresse anzugeben!

Was ist Phishing?

Phishing ist einer der häufigsten auf E-Mail basierenden „Social Engineering“ Angriffe. Mit dieser Technik versuchen Cyber-Kriminelle, Sie zu Aktionen zu verleiten oder Ihnen Informationen zu entlocken.

Wie können Sie Ihr E-Mail-Konto gegen Gefahren schützen?

- Die goldene Regel – Je öffentlicher Ihre E-Mail-Adresse wird, desto mehr SPAM und Phishing E-Mails erhalten Sie.

- Richten Sie für verschiedene Zwecke verschiedene E-Mail-Konten ein.
  - Private Nachrichten
  - Kommunikationslisten
  - Werbung
  - Einmalige Käufe
  - Online-Shopping

- Registrieren Sie sich nur, wenn es wirklich notwendig ist. Vermeiden Sie Last Minute-Angebote, bei denen Sie Ihre “Visitenkarte“ hinterlassen sollen.

- Wenn Sie sich irgendwo mit Ihrer E-Mail-Adresse registrieren, sollten Sie PASSWÖRTER IMMER NUR EINMAL BENUTZEN.

Passwörter – Hierauf sollten Sie achten

- Passwörter († RIP)
  - Immer nur einmal verwenden!
  - Kriminelle führen Skripte aus, mit denen sie unterschiedliche Webseiten auf Benutzernamen und Passwörter überprüfen können.
  - Auch wenn Sie für sich diese Risiken eingehen, was ist, wenn einer Ihrer Provider gehackt wird?
  - Haben Sie Ihr Passwort schon einmal in einem Internetcafé, Hotel oder einem andern gemeinsam genutzten Computer eingegeben? Dann ist es sehr gut möglich, dass Ihre Zugangsdaten bereits in kriminelle Hände gelangt sind.

So schützen Sie Ihre Passwörter

- **Niemals** und unter keinen Umständen Passwörter mehrfach benutzen.

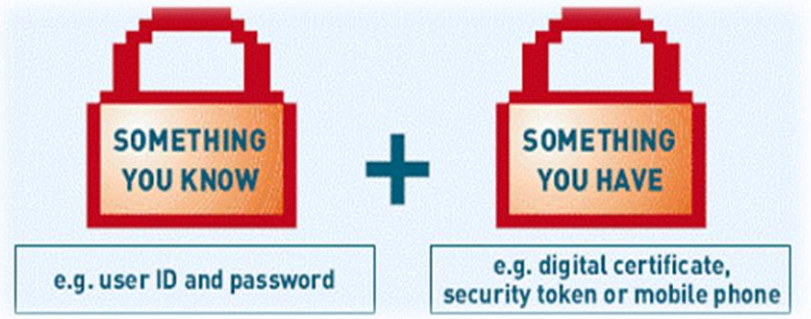
- Bei der Anmeldung zu einem Online-Service immer auf eine **Zwei-Faktor-Authentifizierung** achten (einmalig vergebenes Passwort, Anrufe, SMS oder auch E-Mails an ein zweites Konto).

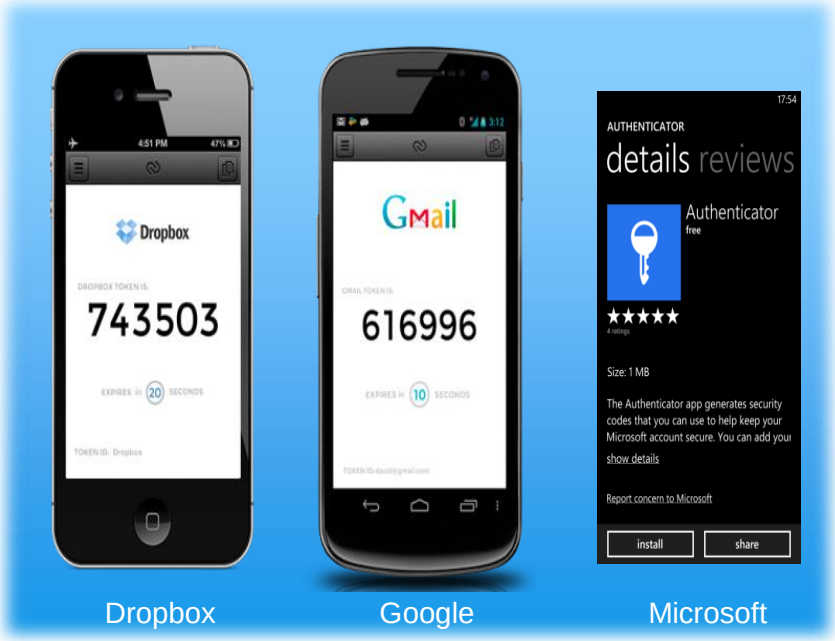
- Die Nutzung eines Passwörter-Verwalters kann nützlich sein, wenn mittels „Advanced Encryption“ verschlüsselt und Ihr Passwort dabei nicht im Internet hin- und her befördert wird.

- Denken Sie daran, auch Ihre Smart-Geräte (Handy, Tablet etc.) mit einem Passwortschutz zu versehen.

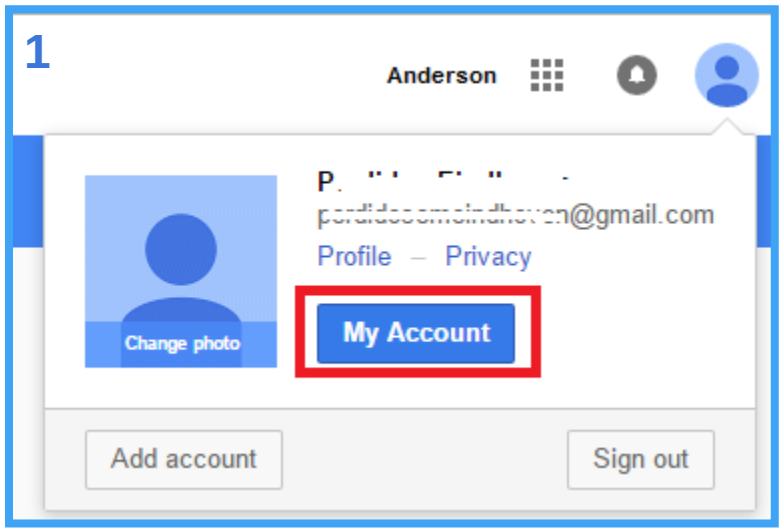
Schützen Sie Ihr E-Mail-Konto mit Hilfe der Zwei-Faktor Authentifizierung

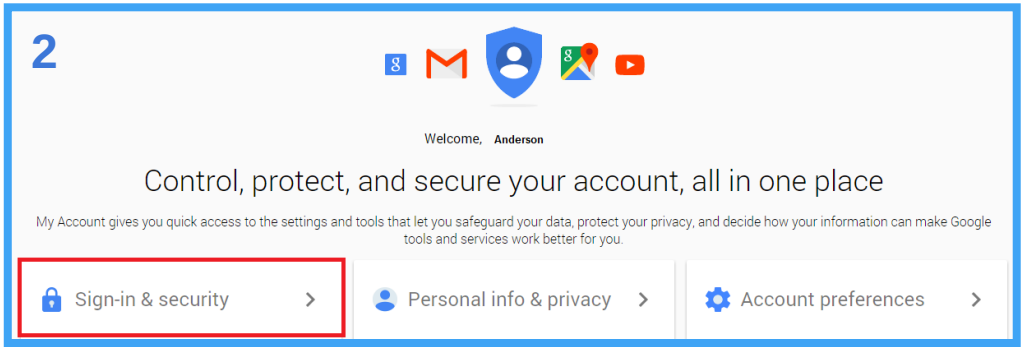
- Wenn Sie sich bei Ihrem E-Mail Provider einloggen, müssen Sie sich normalerweise mit nur **einem Faktor authentifizieren**, in der Regel ist dies ein bestimmtes Kennwort, das Ihr Passwort ist.
- Erhält ein Hacker Zugriff auf Ihr Passwort kann er mit ziemlicher Sicherheit auch auf Ihre E-Mails zugreifen, es sei denn…

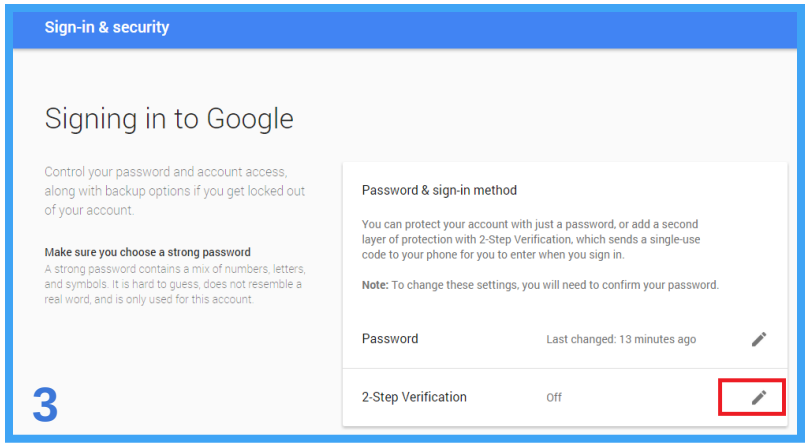


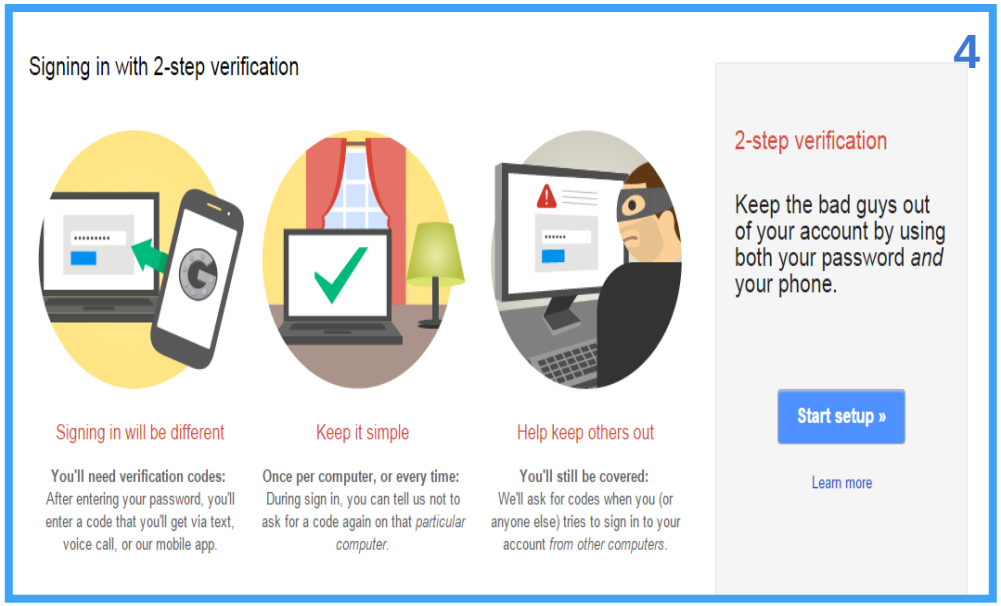


Aktivierung der Google 2-Faktor-Authentifizierung Schritt-für-Schritt erklärt

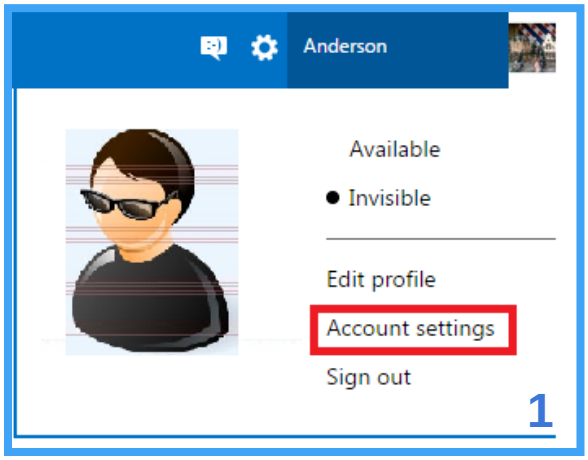


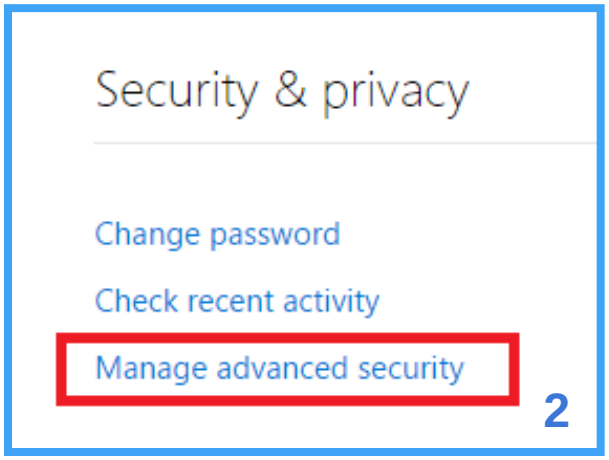


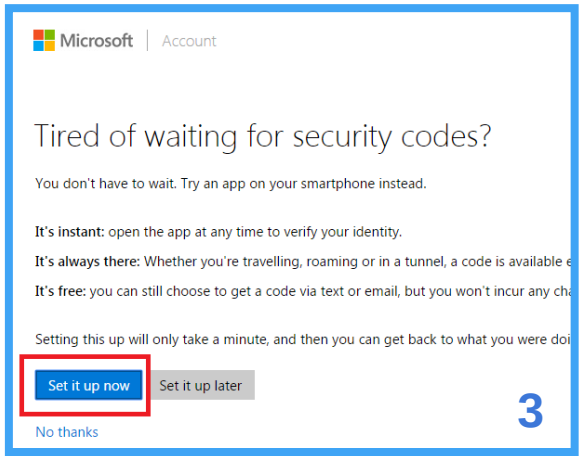


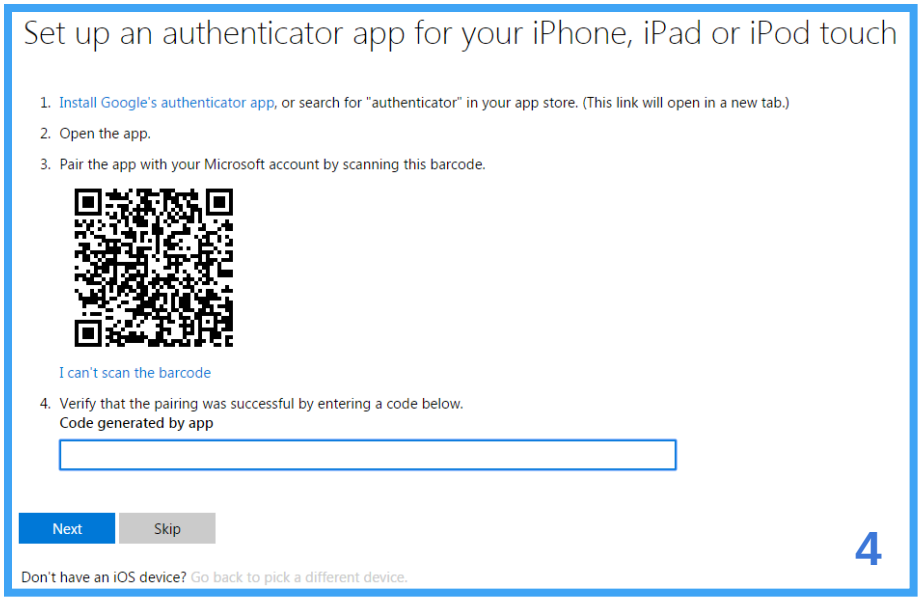


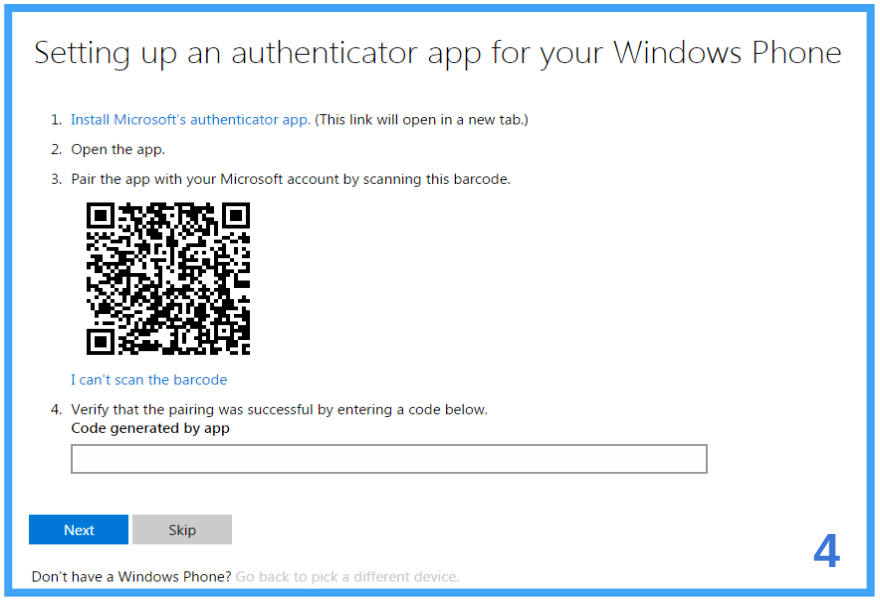
Aktivierung der Google 2-Faktor-Authentifizierung Schritt-für-Schritt erklärt











Konkrete Gefahren bei Heimcomputern

- Ein Computer mit mehreren Nutzern bietet folgende Gefahren:
  - Können verschiedene Personen darauf zugreifen, müssen auch verschiedene Sicherheitsstufen vorhanden sein;
  - Erwiesenermaßen nutzen Kriminelle das Herunterladen von Raubkopien sowie den Besuch von Spiele- und Erotik-Webseiten häufig, um Virus- und Schadprogramme zu installieren.
  - Vertrauen Sie dem Computer Ihres Freundes? Schützt er seinen Computer ebenso gut wie Sie selbst?

- Vorsicht beim Anschließen von fremden Speichergeräten oder DVDs. Es passiert immer noch sehr häufig, dass ein Computer über einen USB Stick mit einem Virus infiziert wird.

Vielseitig verwendbar… aber nicht uneingeschränkt

≠

Wie können Sie Ihren Computer gegen Gefahren schützen?

- Trennen Sie Arbeit und Freizeit; wenn Sie Ihren Computer für Beruf und Freizeit nutzen, gehen Sie ein großes Risiko ein. Das Gleiche gilt auch für mobile Geräte.
- Computer nur alleine nutzen! Wenn einer einen Fehler macht, hat der andere automatisch auch ein Problem. Dies gilt auch für Computer bei Konferenzen, in Hotels und Internetcafés.
- Kaufen Sie eine umfassende Sicherheitslösung (Firewall, Antivirus, AntiSpam) und aktivieren Sie automatische OS (Windows, Android, Mac OSX, oder Linux XYZ) Updates.
- Vermeiden Sie es, Software von unbekannten Quellen oder Freunden herunterzuladen oder zu erwerben.
- Halten Sie Ihre Computersoftware immer auf dem neuesten Stand und installieren Sie die erforderlichen Patches und Antivirus-Updates.

Sicherheit im Internet

Sie haben es in der Hand!

Fangen Sie noch heute damit an.

Autoren: Anderson Domingues (LBR) & Suzanne Jurczik (LBR)