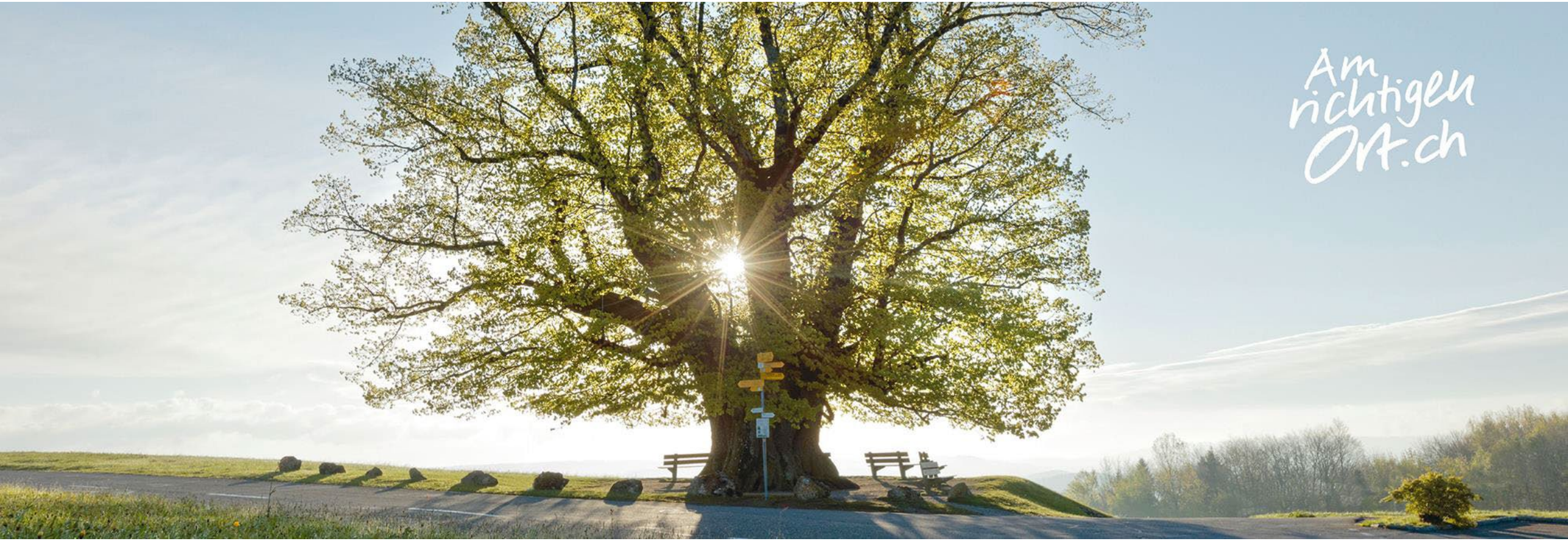
e-Banking, aber sicher?

Ja, sicher!



Agenda

- Grundsatz: Wer Respekt hat, braucht keine Angst zu haben
- Grundregeln im Umgang mit e-Banking und Mobile Banking
- Mögliche Betrugsfälle und wie Sie diese vermeiden können
- Login und Zugangsdaten
- Zwei-Faktor-Authentisierung zur Ihrer Sicherheit
- Weitere nützliche Informationen

Grundsatz: Mit Respekt und ohne Angst!

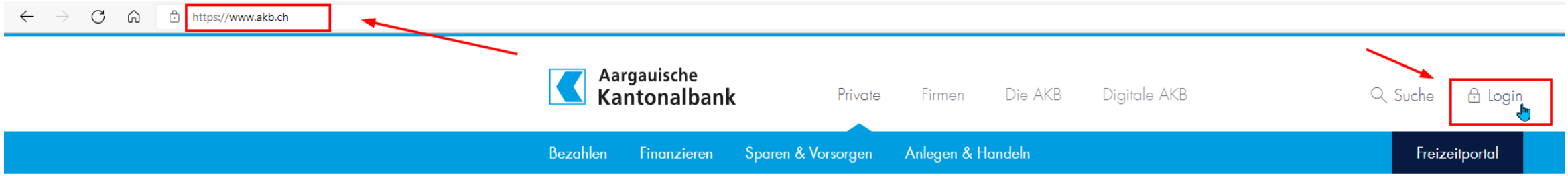
- Beim Beachten von Grundregeln ist Angst nicht nötig und auch kein guter Begleiter.
- Respekt ist durchaus angebracht und fördert, sich angemessen mit der Materie auseinander zu setzen.

Grundregeln im Umgang mit e-Banking und Mobile Banking

- Schützen Sie Ihre Geräte mit einer Sicherheitssoftware (Virenschutz)
- Sicheres Anmelden im e-Banking bzw. Mobile Banking
- Vorbeugen mit Softwareupdates
- Ihre Geräte mit PIN bzw. Passwort vor unbefugtem Zugriff schützen
- Sauberes Abmelden
- Aufpassen und wachsam sein – gesunder Argwohn

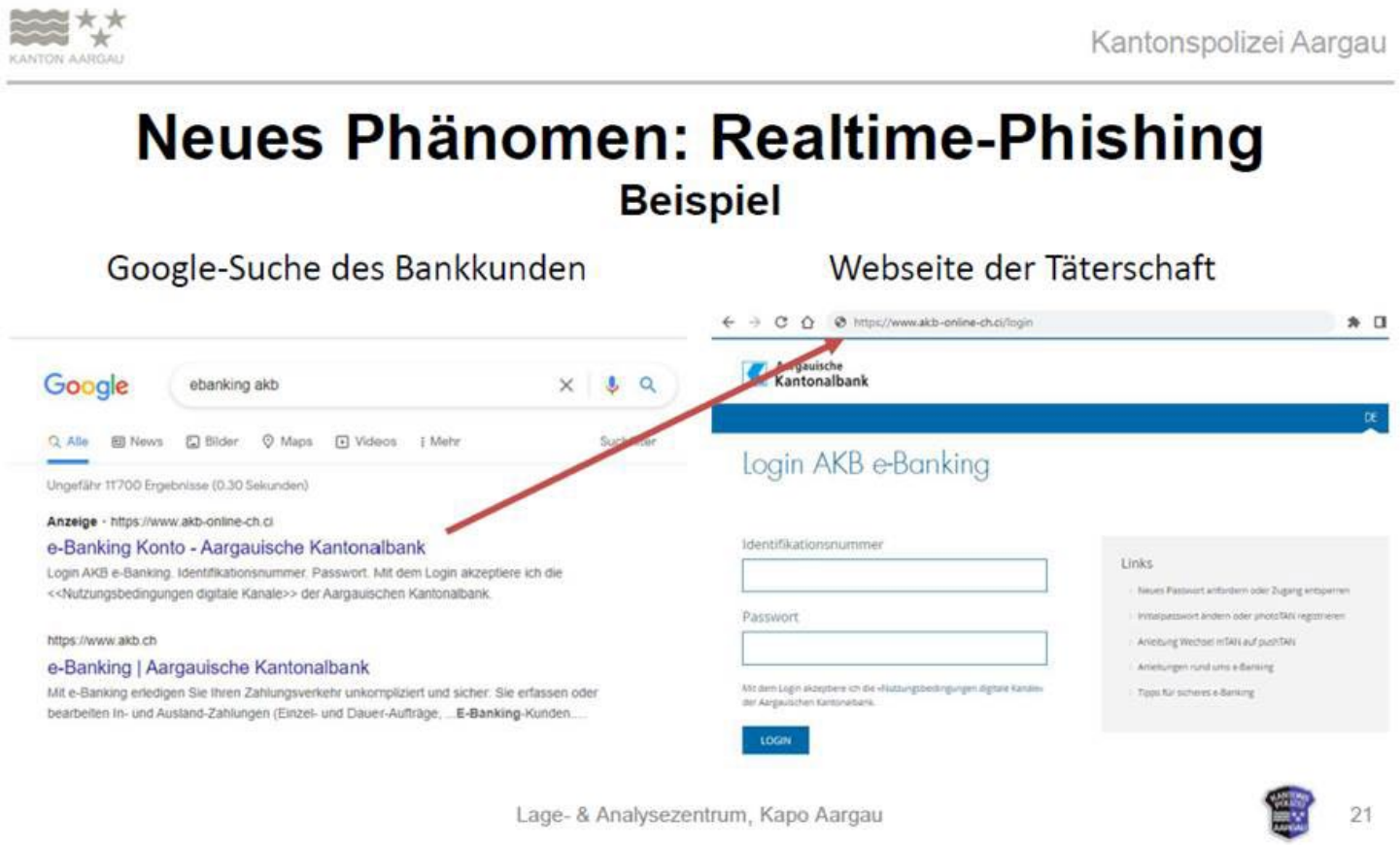
Mögliche Betrugsfälle und wie Sie diese vermeiden können

Login immer über die Website der Bank mittels Aufruf in der Adressleiste im Webbrowser



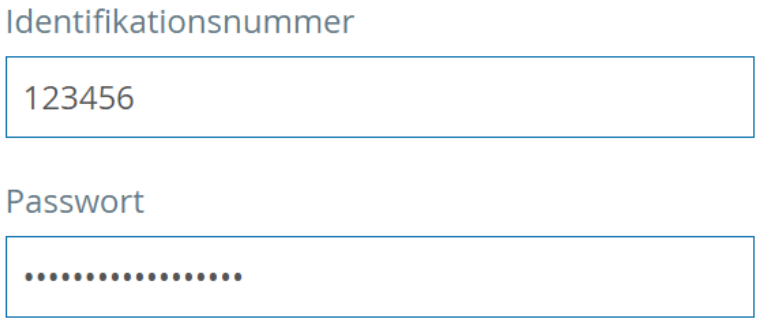
- Google oder Suchmaschinen sind nützlich, nicht jedoch für e-Banking.
- Über Suchmaschinen können betrügerische Login Seiten angezeigt werden, die derjenigen der Bank exakt gleichen und womit die Zugangsdaten abgegriffen werden.

Mögliche Betrugsfälle und wie Sie diese vermeiden können



Mögliche Betrugsfälle und wie Sie diese vermeiden können

Geben Sie niemals online, telefonisch oder persönlich Logindaten bzw. andere sensible Daten an Dritte weiter. Erteilen Sie niemals Zugriffe auf Ihre Geräte.



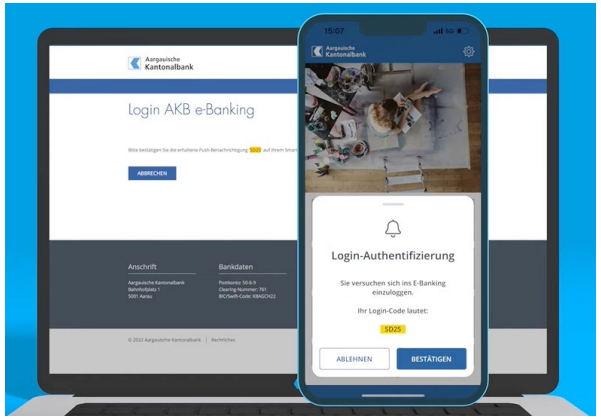
- Banken fragen niemals nach Ihren Logindaten!
- Erteilen Sie niemandem Zugriff auf Ihre Geräte. Auch wenn Anrufende zum Beispiel auf die Dringlichkeit hinweisen und Ihnen vermeintlich helfen wollen.
- Lassen Sie sich nicht einschüchtern. Rufen Sie im Zweifelsfall auf die Hauptrufnummer der Bank an.

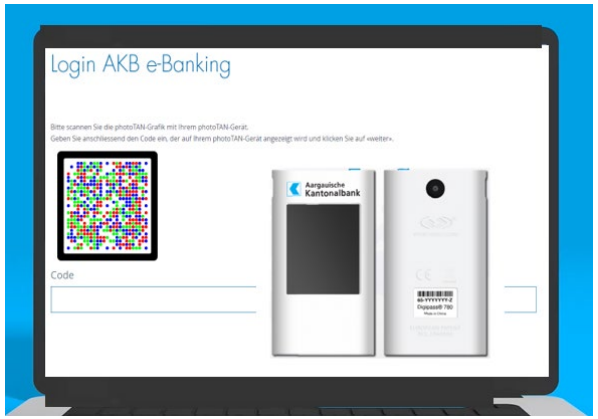
Login und Zugangsdaten

- Verwenden Sie kein Passwort für e-Banking bzw. Mobile Banking, welches auch für andere Online-Zugänge festgelegt wurde.
- Das Passwort sollte kontinuierlich gewechselt werden, Gross- und Kleinbuchstaben, Zahlen sowie Sonderzeichen enthalten und nicht einfach zu erraten sein.
- Geben Sie Ihre Zugangsdaten niemandem bekannt. Wenn diese notiert werden, sollten die Unterlagen unter Verschluss sein.
- Speichern Sie keine Passwörter – insbesondere für e-Banking – in Ihrem Webbrowser.

Zwei-Faktor-Authentisierung: Sicherheit geht vor! pushTAN und photoTAN bei der AKB

- Für den Erhalt des Zusatzcodes (Zwei-Faktor-Authentisierung) bieten Banken verschiedene Login-Verfahren an.
- Die AKB setzt auf pushTAN (Freigabe über das Smartphone). Dabei wird eine push-Mitteilung auf das Smartphone gesendet, die bestätigt werden muss.
- Als alternative Loginmethode wird photoTAN angeboten. Auf dem Computer-Bildschirm wird ein farbiger Code angezeigt. Diesen Code fotografiert man mit einem kleinen Spezialgerät ab und gibt ihn im Webbrowser ein.





e-Banking ist sicher!

Weitere nützliche Informationen

- Die AKB unternimmt höchste Anstrengungen, um die gültigen Sicherheits-Standards zu übertreffen.
- Sie können im AKB e-Banking die Sicherheitsstufe selbständig erhöhen und alle Zahlungen ins Ausland bzw. sämtliche Zahlungen durch einen Zusatzcode freigeben.
- Wer sich an die Grundregeln hält, wird im e-Banking mit Sicherheit auch kein böses Erwachen erleben.
- Die Hochschule Luzern betreibt – in Zusammenarbeit mit diversen Banken in der Schweiz – eine Website über sicheres e-Banking (www.ebas.ch). Dort erhalten Sie Tipps, können Anleitungen einsehen und herunterladen sowie Kurse buchen.

Gerne beantworte ich Ihre Fragen!

Aargauische
Kantonalbank

Am richtigen Ort.ch