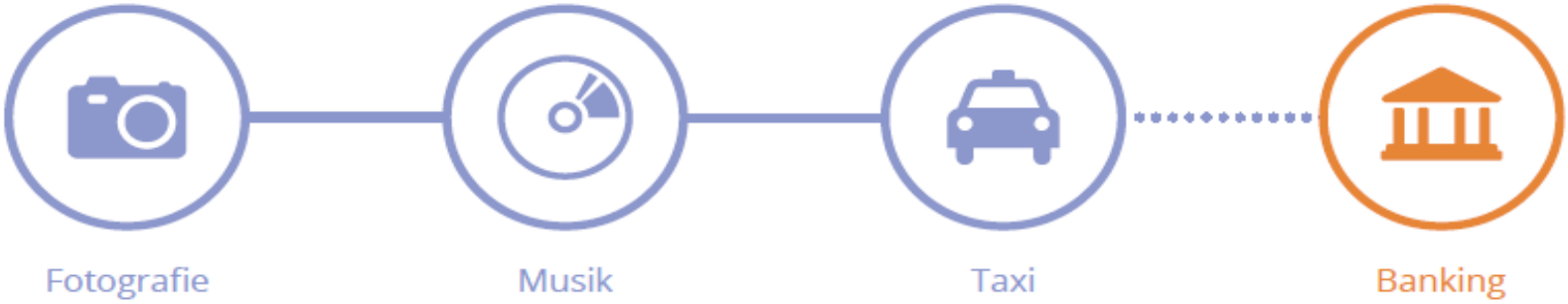
Sicherheit im modernsten Banking Österreichs

George
macht glücklich.

Lena Lakovic
Channel Development

Digitalisierung verändert unser Leben



Digitale Eco-System George


SECURITY

Welche möglichen Bedrohungsszenarien gibt es?

Phishing-Attacken - Was ist Phishing?

Kriminelle können gefälschte E-Mails aussenden, die den E-Mails Ihrer Bank sehr ähnlich sind. Dabei können über Links oder Anhänge in der E-Mail Ihre Zugangsdaten für digitales Banking abgefragt werden.

Kriminelle können sich täuschend echt als Bankmitarbeiter ausgeben und am Telefon um Ihre Zugangsdaten, wie die Verfügernummer, das Passwort, einen TAC oder eine TAN, bitten.

Durch Phishing-Attacken können Kriminelle an Ihre Identifikationsmerkmale gelangen, in der Folge Ihre Identität annehmen und finanzielle Transaktionen in Ihrem Namen durchführen. Sie selbst erfahren von dieser kriminellen Handlung erst, wenn der finanzielle Schaden bereits eingetreten ist.

ERSTE SPARKASSE

Schadprogramme / Trojaner - Malware und Trojaner?

Über sogenannte Schadprogramme (Malware) oder Trojaner können sich Kriminelle trotz moderner Sicherheitstechnologie zum Beispiel in die Kommunikationskanäle zwischen Ihnen und Ihrer Bank schalten und sensible Bankdaten abfangen. Wir empfehlen Ihnen daher grundsätzlich **s Kontakt** (in George oder als eigene App) als sicheren Kommunikationskanal zu Erste Bank und Sparkasse.

Gefälschte Webseiten sind regelmäßig im Umlauf. Diese fordern Sie zum Beispiel auf, ein „Telefon-Sicherheitsmodul“ auf Ihrem Smartphone zu installieren. Dabei werden Details zu Ihrem Smartphone abgefragt. Per SMS wird dann ein Schadprogramm an die angegebene Handy-Nummer geschickt. Dieses Programm kann dann SMS-Nachrichten unbemerkt an Dritte weiterleiten.

ERSTE SPARKASSE

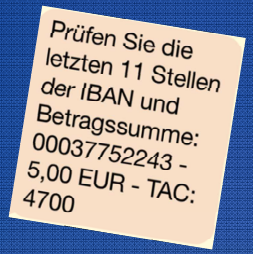
Cybercrime Prevention

Seien Sie aufmerksam!

1. netbanking-/George-Zugangsdaten (Passwort, TAC-SMS, TAN) vor fremden Zugriff schützen und niemals weitergeben

2. Sicherheitshinweise im Sicherheits Center und die Sicherheitswarnungen im Digitalen Banking ernst nehmen

3. TAC-SMS-Verfahren verwenden und Zahlungs-Daten in SMS prüfen – Daten sind nicht OK?



4. Unbekannte Seiten werden in George / netbanking angezeigt?

5. Im Namen der Bank werden geheime Zugangsdaten per E-Mail oder Telefon abgefragt?

ERSTE SPARKASSE

5. Verwenden Sie immer den aktuellen Virenschutz für Ihren PC/Lap Top

Android Virenschutz zum Vorteilspreis für Erste-Kunden

6. Schützen Sie speziell Android-Smartphones → http://ebspk.ikarus.at

7. Öffnen Sie keine unbekannten E-Mails

8. Laden Sie unsere Apps NUR aus den offiziellen stores der Hersteller
→ Apple Store / Google Play Store

9. Verwenden Sie für das Digitale Banking nur Smartphones
die nicht gejailbreakt oder gerootet sind

„mit gesundem Hausverstand statt sorglos agieren“

ERSTE SPARKASSE

George Sicherheitsmerkmale nutzen

s Kontakt – George / App sicheren Kommunikationskanal nutzen

Was tun, wenn Sie irrtümlich Daten bekannt gegeben haben oder einen Missbrauch feststellen?

Help ?

Sicherheits Center auf sparkasse.at oder 050 100 + BLZ (24h)

ERSTE SPARKASSE

Jetzt wird aus Banking Smiling.

...für 500.000 George User