KURZFASSUNG LEITFADEN PHISHING

Unautorisierte Zahlungen mit digitalen Debitkarten und Online-Überweisungen

WAS SOLL/KANN ICH ALS KUNDE SELBST TUN?

Vorbeugende Maßnahmen:

- Push Nachricht im hausbanking für Kontoausgänge
  > hausbanking > Benutzerkonto Rosemarie Musterfrau > Mitteilungs-Einstellungen
- Regelmäßige Überprüfung der gebundenen Geräte
  > hausbanking > Benutzerkonto Rosemarie Musterfrau > Sicherheit > gebundene Geräte
- Hausbanking immer über die Homepage www.vbnoe.at öffnen
- Einstieg ins hausbanking bevorzugt über eigenes sicheres WLAN (Vorsicht im Ausland oder bei öffentlichen Hotspots in Städten, Zügen)
- Eingehende Mails prüfen
  > Prüfung der Absender Mailadresse
  > keine Links anklicken
  > keine Daten bekannt geben
- Achten auf eine sichere Umgebung beim Surfen im Internet
  > auf sichere Internetseiten achten: https:// und Schlosssymbol
  > in der Internetadresse kommt der offizielle Firmenwortlaut vor

Adhoc Maßnahmen:

- **Transaktionssperre oder Benutzersperre**
  > hausbanking > Benutzerkonto Rosemarie Musterfrau > Sicherheit > sperren
  NEU auf Ihrer App-Login Startseite: Einstieg direkt zum Menü über den Button „Sperren“
- **Sperre Debitkarte** (Bankomatkarte) - physische Karte inkl. digitale Karten
  ACHTUNG: Um eine eindeutige Identifikation zu gewährleisten benötigen Sie für die Sperre Ihren IBAN und die Bankleitzahl.
  > Kundenservice Center der VBNÖ Tel.Nr. 02742/391-0
  Mo-Do 08:00-16:30 Uhr
  Fr 08:00-17:00 Uhr
  > Sperrtelefon der Payment Services Austria Tel.Nr. 0800/2048800
  Mo-So 0:00-24:00 Uhr
- **Sperre der Kreditkarte** PayLife 05/99064500
- Wurde der Benutzer durch den Angreifer aus dem hausbanking ausgesperrt, kann er durch die Eingabe seines Benutzernamens und mehrfache Eingabe eines falschen Passwortes ein Soft-Lockout in Gang setzen.
- Bei Betrugsfall alle Daten als Beweis sichern, die in Zusammenhang mit dem Phishing-Vorfall stehen
  > Mail oder SMS
  > polizeiliche Anzeige erstatten