03.03.2022

Wie man Bankbetrüger in den Wahnsinn treibt

Cyberkriminelle wenden immer neue Methoden an, um an das Geld ihrer Opfer zu gelangen. In diesem Zusammenhang ein Hinweis zu einem Video, welches auf eine aktuelle Gefahr mit viel Humor aufmerksam macht.

Trotz des Unterhaltungswertes des Videos wird auf eine sehr aktuelle Methode der Cyberkriminellen eingegangen – sehen Sie selbst: www.youtube.com/watch?v=8_5eQw-kdyM (http://www.youtube.com/watch?v=8_5eQw-kdyM)

Schutz vor der im Film angesprochenen Gefahr, bei der die Adresse des Finanzinstituts im Google-Suchfenster eingegeben wird, um zum E-Banking-Portal zu gelangen, bieten folgende Massnahmen:

- Tippen Sie die Adresse Ihres Finanzinstituts immer von Hand direkt in der Adresszeile des Browsers ein – und nicht im Google-Suchfenster!
- Tippen Sie nie «Login meineBank» oder «E-Banking meineBank» oder ähnliches im Google-Suchfenster ein. Google zeigt Anzeigen (auch von Betrügern!) vor den eigentlichen Suchresultaten an. Klicken Sie niemals auf solche Anzeigen, falls diese Ihr Finanzinstitut erwähnen.
- Achten Sie auf eine sichere Verbindung (Schloss-Symbol, richtiger Name des Finanzinstituts und korrekter Domänen-Name).

Im Film ebenfalls angesprochen wird der Remote-Support. Dabei handelt es sich um eine Technologie, um fremde Hilfe auf das eigene Gerät zu holen, ohne dass ein Techniker vor Ort sein muss. Auch Finanzinstitute nutzen im Rahmen ihres Supports bzw. Helpdesks diese Möglichkeit. Beachten Sie bei der Nutzung dieser Technologie folgende Massnahmen:

- Rufen Sie keine Telefonnummern des Supports bzw. Helpdesks an, die Ihnen bei Google-Anzeigen angezeigt werden.
- Stellen Sie Verbindungen nur mit vertrauenswürdigen Personen her. Seien Sie insbesondere zurückhaltend, falls Sie nicht der Initiant der Verbindung sind.
- Verwenden Sie eine sichere Verbindung (Schloss-Symbol, richtiger Name des Finanzinstituts und korrekter Domänen-Name).
- Gewähren Sie keinen Vollzugriff auf Ihr System. Die Person, die Ihnen hilft, sollte nur passiv zusehen können.
- Beachten Sie, dass alles, was auf dem Bildschirm erscheint, vom Gegenüber gesehen und auch aufgezeichnet werden kann.
- Surfen Sie nicht auf Internetseiten, die nichts mit der Sitzung zu tun haben – auch wenn Sie dazu angewiesen werden.
- Stellen Sie sicher, dass nach Inanspruchnahme der Hilfeleistung die Remote-Support Verbindung beendet wird, um weitere Zugriffe auf Ihr Gerät zu unterbinden.