Veröffentlicht auf www.leineblitz.de am Freitag, 14.01.22 um 09:31 Uhr:

110 & 112: Polizei warnt vor falschen Microsoft-Mitarbeitern am Telefon

REGION. Falsche Microsoft-Mitarbeiter am TelefonDas Phänomen ist nicht neu, aber leider immer wieder aufs Neue aktuell. Falsche Microsoft-Mitarbeiter, die arglose Bürger um ihr Geld zu bringen versuchen. Gerade jetzt, wo erneut viele Kontakte und Erledigungen von der "normalen" in die Onlinewelt verlegt werden, nutzen Betrüger die Hilfsbereitschaft, aber auch das nicht immer umfassende Wissen um die Sicherheit im Netz vieler Mitbürgerinnen und Mitbürger schamlos aus.

Den Opfern wird, meistens durch einen Anruf auf die Festnetznummer, suggeriert, es gebe einen Hackerangriff oder ein Virus auf ihren Computer oder ihr Smartphone. Dies ermögliche Kriminellen zum Beispiel Zugriff auf das Onlinebanking der Betroffenen. Natürlich haben der oder die freundlichen und äußerst hilfsbereiten Anrufer eine Lösung für dieses Sicherheitsproblem parat: sei es die Installation einer bestimmten (Schad)Software, oder die Einrichtung eines Fernzugriffs auf das betroffene Gerät, um die Sicherheitslücke zu schließen.

Zur Überprüfung des Erfolgs werden nun die Opfer zur Durchführung von sogenannten Testüberweisungen ermutigt, bei denen sie zuvor auf ihrem Konto gutgeschriebene Beträge,teilweise in vierstelliger Höhe, weiterüberweisen sollen.Leider handelt es sich bei den angeblichen Gutschriften nicht um real getätigte Überweisungen, so dass letzten Endes das Konto der Opfer um eben diesen Betrag erleichtert wird.

Im schlimmsten Fall wurden die Opfer dazu gebracht, mit ihren eigenen Daten ein Konto bei einer von den Betrügern vorgegebenen Bank zu eröffnen. Dieses Konto wird im Anschluss von den Betrügern genutzt, um weitere Opfer um ihr Erspartes zu bringen, nur dass sich nun der Eröffner des Kontos plötzlich polizeilichen Ermittlungen ausgesetzt sieht, da seine Daten und sein Konto zur Begehung von Straftaten verwendet wird.

Wie können Sie sich vor derartigen Anrufen schützen?

- Lassen Sie ihren Telefonbucheintrag, wenn vorhanden, ändern oder löschen.
- Reagieren Sie grundsätzlich bei unbekannten Anrufern misstrauisch und beenden Sie das Gespräch umgehend, wenn Ihnen etwas merkwürdig vorkommt.
-Halten Sie Virenschutzprogramme auf ihrem Computer und Smartphone immer auf dem aktuellsten Stand, so müssen Sie sich keine Gedanken um angebliche Hackerangriffe machen.
- Lassen Sie sich nicht aus Unkenntnis Computerprobleme einreden.
- Geben Sie niemals Zugangsdaten oder Passwörter heraus und lassen Sie nicht per Fernzugriff Software auf ihrem Computer installieren.
- Lassen Sie sich nicht zur Eröffnung eines Kontos überreden.
- Geben Sie keine persönlichen Daten wie Personalien oder Ausweisdaten bekannt. Diese können ebenfalls von den Betrügern zur Eröffnung von Konten oder Kundenkonten unter Ihrem Namen verwendet werden.
- Sprechen Sie in ihrem Freundes- und Familienkreis über das Thema.
- Bei Zweifel oder Unsicherheiten informieren Sie sich bei ihrer örtlichen Polizeidienststelle oder unter www.polizei-beratung.de.

von Redaktion LeineBlitz