Tipps und vorbeugende Massnahmen zur Einschränkung des Risikos eines Verlusts sensibler Daten durch Phishing-Kampagnen und/oder Geräteinfektionen durch Malware und Trojaner

1. Best Practices für die Sicherheit von Smartphones

- Verwenden Sie komplexe Passwörter, auch zum Entsperren des Smartphones und für den Zugriff darauf (siehe Abschnitt 3).
- Konfigurieren Sie die automatische Sperre des Smartphones (nach Zeit oder Inaktivität).
- Aktivieren Sie den biometrischen Zugriff.
- Sichern Sie regelmäßig den Inhalt des Smartphones, um wichtige Daten zu erhalten.
- Vermeiden Sie die Nutzung inoffizieller Smartphone-Händler oder -Reparaturdienste.
- Installieren Sie nur die Originalsoftware.
- Halten Sie die Smartphone-Software auf dem neuesten Stand.
- Halten Sie die Anwendungsversionen auf dem neuesten Stand.
- Seien Sie vorsichtig bei Nachrichten (SMS oder E-Mail) sowie Anrufen von unbekannten Nummern oder aus nicht vertrauenswürdigen Quellen, bei denen personenbezogene Daten abgefragt werden, sei es telefonisch oder über Links, bei denen die Domain nicht klar und eindeutig identifizierbar ist.
- Konfigurieren Sie das Gerät mithilfe der Betriebssystemoptionen richtig, um die Installation von Anwendungen aus unbekannten Quellen zu verhindern.
- Im Falle eines Diebstahls Ihres Geräts, melden Sie dies bitte BBVA und rufen Sie den entsprechenden Betreiber an, um die SIM-Karte und das Smartphone sperren zu lassen. Wenn Sie den Dienst „Remote Information Deletion“ haben, wird empfohlen, ihn zu verwenden.
- Aktivieren Sie Bluetooth am Mobiltelefon nur, wenn es unbedingt nötig ist, und vermeiden Sie die Verbindung zu unbekannten Bluetooth-Geräten.
- Fordern Sie immer eine Autorisierung an, wenn jemand versucht, eine Verbindung zu Ihrem Gerät herzustellen.

- Stellen Sie sicher, dass Bluetooth im Modus „Ausgeblendet“ ist, und vermeiden Sie das Koppeln von Bluetooth-Geräten an öffentlichen Orten, da über diesen Kommunikationskanal verschiedene Arten von Angriffen (z. B. Bluejacking, Bluebugging, Bluesnarfing) stattfinden.
- Aktivieren Sie Internetverbindungen über WLAN nur, wenn es unbedingt nötig ist, und vermeiden Sie Verbindungen zu unbekannten Zugangspunkten, da alle Informationen, auch vertrauliche Informationen, wie Gespräche, Passwörter, Bankdaten usw., vom Besitzer des Zugangspunkts, über den Sie eine Verbindung zum Internet herstellen möchten, abgefangen werden können.
- Trennen Sie die Verbindung zu Webdiensten, die ein Kennwort erfordern, oder melden Sie sich ab, bevor Sie den Browser schließen.
- Wenn das Betriebssystem die Verfügbarkeit einer neuen Version des Systems selbst oder neuer Updates der auf dem Gerät installierten Anwendungen meldet, akzeptieren und installieren Sie diese, da sie häufig Funktionen hinzufügen und Sicherheitslücken beheben und so mögliche Infektionen durch das Vorhandensein anfälliger Anwendungen auf dem Telefon verhindern.
- Wenn Sie das Smartphone entsorgen möchten, empfiehlt es sich, zunächst dessen Inhalte zu löschen, um zu verhindern, dass Dritte auf die darauf gespeicherten Informationen wie Kontakte, SMS, Fotos, E-Mail-Konten, Anwendungen für den Zugriff auf soziale Netzwerke, Online-Shops oder Zahlungsgateways, den Cache und im Browser gespeicherte Passwörter zugreifen. Es wird empfohlen, das Gerät neu zu formatieren und, sofern das Betriebssystem dies zulässt, die Funktion zum Zurücksetzen auf die Werkseinstellungen (Wiederherstellen und Löschen) zu verwenden.
- Misstrauen Sie E-Mails, in denen biometrische Daten durch das Senden von Fotos oder Videos angefordert werden.
- Installieren Sie ein mobiles Antiviren-/Antimalware-Programm.
- Aktivieren Sie die Fernlokalisierung, Fernblockierung und Fernlöschung bei Verlust oder Diebstahl des Geräts.

2. Was tun, wenn das Gerät infiziert ist oder ein Infektionsverdacht besteht

- Analysieren Sie das Vorhandensein anomaler Dateien oder Ordner mithilfe eines Antivirenprogramms, um alle auf dem Gerät vorhandenen Viren zu identifizieren und zu beseitigen.
- Führen Sie einen Antiviren-/Antimalware-Gerätescan durch.

- Da das Antivirenprogramm nicht immer alle Arten von Malware oder Trojanern erkennen kann, wird empfohlen, das Gerät auf den ursprünglichen Werkszustand zurückzusetzen.
- Ändern Sie die Zugangsdaten für die auf dem Gerät installierten Anwendungen, bevor Sie es formatieren und auf den Werkszustand zurücksetzen.
- Überprüfen Sie die Anwendungen, die Sie auf dem Gerät neu installieren möchten. Stellen Sie dabei sicher, dass diese Anwendungen notwendig sind, aus offiziellen App-Stores stammen und von anerkannten Entwicklern veröffentlicht wurden. Vergewissern Sie sich außerdem, dass diese Anwendungen nur Berechtigungen für das Gerät und personenbezogene Daten erfordern, die für das Funktionieren solcher Anwendungen unbedingt erforderlich sind.

3. Passwörter

- Bevor Sie neue Passwörter für die Anwendungen festlegen, scannen Sie das Gerät mit einem Antivirenprogramm, um das Vorhandensein von Malware oder Trojanern festzustellen, die möglicherweise auf dem Gerät installiert sind.
- Passwörter sollten mindestens acht Zeichen lang sein. Je länger das Passwort, desto schwieriger ist es zu entschlüsseln und desto mehr Sicherheit bietet es.
- Bereits verwendete Passwörter sollten nicht wiederverwendet werden.
- Bilden Sie Passwörter mit einer Kombination aus alphabetischen Zeichen (Groß- und Kleinbuchstaben), Ziffern und Sonderzeichen (@, +, &).
- Verwenden Sie je nach Verwendungszweck unterschiedliche Passwörter (verwenden Sie beispielsweise nicht dasselbe Passwort für ein E-Mail-Konto und für den Zugang zu Bankdienstleistungen).
- Eine gute Methode zum Erstellen eines komplexen Passworts besteht darin, sich eine leicht zu merkende Phrase auszudenken und diese durch die Anwendung einer einfachen Regel zu verkürzen.
- Passwörter sollten regelmäßig geändert werden.
- Das Passwort sollte nicht den Benutzernamen des Kontos oder andere leicht identifizierbare persönliche Informationen (Geburtstage, Namen der Kinder, Ehepartner usw.) enthalten. Vermeiden Sie außerdem aufeinanderfolgende Buchstabenfolgen auf der Tastatur (qwertz) oder in alphabetischer bzw. numerischer Reihenfolge (123456, abcde usw.).

- Vermeiden Sie Passwörter, die Wörter enthalten, die in einer bestimmten Sprache existieren (z. B. „Feld“). Einer der bekanntesten Angriffe zum Knacken von Passwörtern besteht darin, jedes Wort in einem Wörterbuch und/oder häufig verwendete Wörter zu testen.
- Passwörter sollten nicht an einem öffentlichen Ort oder in Reichweite Dritter aufbewahrt werden (auf dem Tisch, auf Papier geschrieben usw.).
- Geben Sie Passwörter nicht über das Internet (per E-Mail) oder per Telefon weiter. Seien Sie insbesondere bei E-Mails misstrauisch, in denen Sie zur Preisgabe der Passwörter aufgefordert werden oder in denen angegeben wird, dass Sie eine Website besuchen sollten, um die Passwörter zu verifizieren. Es handelt sich dabei mit ziemlicher Sicherheit um Betrug.
- Verwenden Sie biometrischen Zugang, biometrische Authentifizierung oder eine offizielle Zwei-Faktor-Authentifizierung.