M.M.WARBURG & CO
BANK

Warnung vor Cyber-Kriminalität

Die Digitalisierung schreitet rasant voran, damit entstehen ständig neue Angriffsmöglichkeiten und das potentielle Risiko von Cyber-Angriffen steigt.

Schützen Sie sich vor Cyber-Kriminalität

Betrugsversuche über digitale Kommunikationskanäle nehmen kontinuierlich zu und erfordern daher unverändert hohe Achtsamkeit. Technische, regulatorische sowie anwendungs-individuelle Rahmenbedingungen werden von den Cyber-Kriminellen zusehends zeitnah adaptiert. Immer neue, mitunter auf Ausspähung persönlicher Verhaltensmuster oder Daten basierende Methoden erfordern einen konstant besonnenen und wachsamen Umgang mit digitalen Kanälen und den benötigten Zugangsdaten.

Phishing: Zugangsdaten via E-Mail ausgespäht

Beim sogenannten Phishing werden Betroffene z. B. über einen Link in einer E-Mail oder Kurznachrichten auf eine authentisch aussehende Internetseite geleitet, die die Daten nach der Eingabe direkt an die Betrüger sendet oder aufgefordert, sensible Daten per E-Mail an eine gefälschte E-Mail-Adresse zu senden.

Spear-Phishing und Pharming: Phishing 2.0

Weiterentwicklungen dieser Methode sind das noch effektivere sogenannte Spear-Phishing, bei dem bewusst eingeflochtene persönliche Daten der Zielperson und ggf. ein gefälschter zusätzlich eingefügter Mailverlauf Zweifel an der Authentizität der Eingabeoberfläche zerstreuen sollen, oder das sogenannte Pharming, das auf der gezielten Manipulation der Domainnamen in Webbrowsern basiert.

Suchmaschinen-Phishing: bleiben Sie bei vertrauten Schritten wachsam

Auch Suchmaschinen werden manipuliert und können arglose Nutzerinnen und Nutzer auf gefälschte Seiten führen, mitunter gleich mit dem ersten Treffer. Oft erscheinen dann vermeintliche Sperrmeldungen oder die Aufforderung zu einer erneuten Installation. Auch hier sollen sensible Daten ausgespäht und später missbräuchlich verwendet werden. Prüfen Sie daher die Adresse Ihres Onlinebanking immer sehr genau oder setzen sich gleich einen Favoriten.

Aktuelle Warnung „Godfather“: Ganze Webseiten werden gefälscht

Aktuell warnt die BaFin für Android-Nutzer vor einer Schadsoftware namens Godfather, die die Dateneingaben von Banking- oder Kryptoanwendungen aufzeichnet. Auch Godfather bedient sich professionell gefälschter Internetauftritte und greift darüber hinaus auf gefälschte Push-Nachrichten zurück, deren Zweck der Zugang zu Authentifizierungscodes ist. Wie genau die Software auf die Endgeräte gelangt, ist dabei noch nicht bekannt.

Betrug am Telefon via Enkeltrick und CEO-Trick

Auch der populäre Enkeltrick (Anruf eines vermeintlichen nahen Verwandten mit der Bitte um kurzfristige Unterstützung in einer Notlage) sowie Varianten desselben werden unverändert angewendet. Gleichfalls immer wieder versucht wird der sogenannte CEO-Trick: Hier setzt Sie eine vermeintlich hochrangige/wichtige Person persönlich unter Druck, Daten preiszugeben und „jetzt keine dummen Fragen zu stellen.“ Auch falsche Bankmitarbeitende oder Polizisten treten immer wieder auf und drängen etwa dazu, Bargeld oder Wertsachen in Sicherheit zu bringen.

Lassen Sie sich nicht unter Druck setzen!

Häufig wird bei diesen Betrugsversuchen künstlich ein hoher Handlungs- und Zeitdruck aufgebaut. Zusehends verbreitet sind auch hybride Formen aus Cyberangriffen und der Aufforderung, sich telefonisch bei einer vermeintlichen Hotline zu melden. Hier erhöhen dann professionell geschulte Personen den Druck, sensible Daten preiszugeben, um etwa einen vermeintlichen Schaden abzuwenden.

Schützen Sie sich und Ihre Daten

Bitte beachten Sie stets: Die Bank und ihre Mitarbeitenden werden Sie niemals dazu auffordern, sensible Zugangsdaten per E-Mail preiszugeben. Seien Sie daher stets achtsam und befolgen Sie die allgemeinen Sicherheitshinweise zum Umgang mit E-Mails z. B. unter https://www.bsi.bund.de/DE/Home/home_node.html

Falls doch etwas passiert ist

Im Zweifel oder wenn Sie bereits sensible Daten weitergegeben haben, setzen Sie sich bitte umgehend mit Ihrer Ansprechpartnerin oder Ihrem Ansprechpartner in der Bank oder unter einer der folgenden Telefonnummern oder E-Mail-Adressen mit uns in Verbindung:

Hotline für Onlinebanking (täglich 6-22 Uhr):
Deutschlandweit kostenfrei: Tel. 0800 72 33 982 / International: Tel. +49 40 3282 2332

Allgemeine bankenübergreifende Sperr-Hotline girocard und Mastercard (rund um die Uhr)
Deutschlandweit kostenfrei: Tel. 116 116 / International: Tel. +49 116 116
E-Mail: service@mmwarburg-service.com

Beachten Sie bitte folgende Hinweise / Sicherheitsempfehlungen:

Halten Sie Ihre Endgeräte auf dem neuesten Stand

Stellen Sie sicher, dass Ihre Firewalls und Virenscanner aktiviert und stets aktuell sind.

Banking Apps nur aus autorisierten App-Stores laden

Zum Laden oder Updaten von Apps für Ihr Smartphone oder Ihr Tablet nutzen Sie bitte ausschließlich die autorisierten App-Stores (Apple: App Store / Android: Google Play Store). Folgen Sie keinen Aufforderungen zum Herunterladen von Apps via E-Mail.

Speichern Sie PINs, TANs und sonstige Zugangsdaten nicht

Kennwörter, persönliche Geheimzahlen (PINs) und Transaktionsnummern (TANs) sollten niemals unverschlüsselt in Apps, der Cloud oder auf der Festplatte abgespeichert werden. Zugangsdaten sollten außerdem regelmäßig geändert werden.

Prüfen Sie die Bank-Webseiten

Prüfen Sie vor einem Login, ob Sie wirklich auf der offiziellen Webseite bzw. im offiziellen Onlinebanking sind. Dies erkennen Sie unter anderem an dem „Schloss"-Symbol im Browser so-wie dem Beginn der URL mit „https". Sollten Sie sich unsicher sein, gehen Sie direkt über unsere Webseite. Unser Onlinebanking finden Sie unter folgendem Link: https://www.warburg-bank.de/#/

Bleiben Sie aufmerksam gegenüber Cyber-Kriminalität!

Grundsätzlich fordern Banken ihre Kunden niemals zur Aktualisierung von sensiblen Daten per E-Mail, SMS oder auch telefonisch auf. Sollte ein vermeintlicher Mitarbeitender einer Bank Sie zu Transaktionen bezüglich Ihres Kontos drängen, beenden Sie das Gespräch umgehend und kontaktieren Sie Ihre Bank direkt.