M.M.WARBURG & CO
BANK

Warnung vor Cyber-Kriminalität

Betrugsversuche über digitale Kommunikationskanäle nehmen kontinuierlich zu und erfordern daher unverändert hohe Achtsamkeit.

Technische, regulatorische sowie anwendungsindividuelle 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 Sie dazu auffordert, 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.

„Godfather“: ganze Webseiten werden gefälscht

Zusätzlich 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.

Aktuelle Warnung: Buchung nicht erfolgreich

Vorsicht vor dieser aktuellen Betrugsmasche: Nach einer Hotel- oder Ticketbuchung auf einem Portal werden Kunden mit einer täuschend echt nachgebildeten Nachricht kontaktiert: Es hätte Probleme mit dem gewählten

Zahlungsmittel gegeben. Für die erneute Eingabe der Zahlungsdaten wird ein Link mitgeschickt oder die Kommunikation auf einen Messenger-Dienst wie WhatsApp umgeleitet. Zugleich wird zeitlicher Druck aufgebaut: Würde man nicht innerhalb einer bestimmten Frist reagieren, wird die Buchung storniert. Vorsicht: Der Link führt auf eine gefälschte Seite, und die Nachrichten stammen von Betrügern. Hierdurch versuchen die Kriminellen, an Zahlungsdaten zu kommen oder den Kunden direkt dazu zu bringen, eine Zahlung auszulösen. Alternativ wird auch eine angeblich notwendige „Verifikation" des Zahlungsmittels gefordert. Folgt der Betreffende den Anweisungen, löst er aber tatsächlich eine Zahlung direkt an die Betrüger aus.

Nutzen Sie für Zahlungen nur genau die Plattform, über die Sie gebucht haben. Lassen Sie sich nicht durch Links auf eine andere Website leiten. Oft ist der Name sehr ähnlich, entspricht aber nicht genau dem ursprünglichen Anbieter.

Reagieren Sie nicht auf Nachrichten Unbekannter, die Sie über Messenger-Dienste bekommen. Machen Sie sich beim Erhalt einer solchen Nachricht bewusst, dass dies nicht der übliche Weg für das Unternehmen ist, Sie zu kontaktieren.

Aktuelle Warnung: Storno einer Zahlung

Gefälschte Storno-Webseiten lauern auf neue Opfer mit diesem Trick: Will jemand eine Buchung stornieren und sucht über eine Suchmaschine nach Informationen dazu, gelangt er oder sie auf eine gefälschte Internetseite. Ruft man die dort angegebene Nummer an, landet man aber direkt bei den Betrügern, die sich als Mitarbeitende des Unternehmens ausgeben und oft nach weiteren sensiblen Informationen fragen. Zudem soll man für eine Rückabwicklung seine bestimmte Anwendung herunterladen und dort die gewünschten Daten hinterlegen. Statt einer Stornierung und Rückerstattung werden aber tatsächlich weitere Zahlungen ausgelöst.

Aktuelle Warnung: TAN-Verfahren aktualisieren

Bankkunden werden aktuell wieder vermehrt mit gefälschten SMS-Nachrichten zum Aktualisieren ihres TAN-Verfahrens getäuscht. In einer von Betrügern versendeten SMS wird darauf hingewiesen, dass die Registrierung für das TAN-Verfahren eines realen Kreditinstituts abgelaufen sei. Die Nachricht enthält einen Link für die angebliche Erneuerung der Registrierung. In Wirklichkeit führt dieser Link zu einer Phishing-Webseite, auf der Kunden ihre Zugangsdaten für Online-Banking oder TAN-App eingeben sollen, die damit in die Hände der Betrüger gelangen. Eine Bank wird niemals per SMS zum Aktualisieren des Sicherheitsverfahrens auffordern.

Aktuelle Warnung: QR-Code-Phishing umgeht Sicherheitssoftware

Schnell einen QR-Code (Quick-Response-Code) scannen und schon gelangt man direkt zur Speisekarte im Restaurant, Anmeldemaske für eine Ticketbuchung oder auf ein Rechnungsformular. Vorsicht: Auch QR-Codes können für Phishing-Angriffe missbraucht werden.

Cyber-Kriminelle schicken etwa eine Mail mit der Aufforderung, einen QR-Code einzuscannen, um ein Dokument oder eine Rechnung zu öffnen. Der Link führt dann auf eine gefälschte Seite, mit dem Ziel, persönliche Daten abzufischen. Oft wird auch hier zeitlicher Handlungsdruck aufgebaut. IT-Sicherheitssoftware wie Anti-Viren-Programme oder die Firewall erkennen solche Phishing-Nachrichten nicht. QR-Codes werden nicht als Anhang, sondern als Bild erkannt.

Auch für QR-Codes gilt jedoch: Diese nur aus vertrauenswürdigen Quellen scannen und im Zweifel den Link nicht öffnen und die geforderten Daten nicht eingeben. Wenn Sie unsicher sind, kontaktieren Sie den Absender auf einem anderen Weg.

Aktuelle Warnung: Cyberkriminelle nutzen KI / Vishing

Sprachprogramme, die mithilfe von künstlicher Intelligenz (KI) wie beispielsweise Chat Bots arbeiten, können Textbausteine innerhalb von Sekunden verarbeiten. Cyberkriminelle nutzen solche Programme, um Phishing-Mails zu korrigieren oder Texte anzupassen, so dass es für den Empfänger noch schwieriger wird, deren Echtheit zu erkennen.

Prüfen Sie im Zweifel die E-Mail-Adresse des Absenders auf Unstimmigkeiten. Alternativ suchen Sie den Absender selbst über einen anderen Zugang der offiziellen Website oder App. Achten Sie darauf, dass die Seite mit **https://** beginnt und auch auf die korrekte Schreibweise einer Ihnen

bereits bekannten Internetseite. Oft verwenden Betrüger eine sehr ähnliche Internetadresse, um Seriosität und Vertrauenswürdigkeit vorzutäuschen. Auch beim so genannten „Vishing“ – das Wort setzt sich zusammen aus den englischen Begriffen Voice und Phishing – nutzen die Betrüger die Möglichkeiten der KI, um Stimmen nahezu perfekt nachzuahmen. Mit Hilfe solch einer Fake-Sprachnachricht soll man dazu verleitet werden, Daten herauszugeben oder gar direkt Geld an die Kriminellen zu überweisen: „Ich hatte einen Auto-Unfall, Du musst mir Geld überweisen.“ „Ihr Konto ist gehackt worden“. Hier muss man sich zwingen, Ruhe zu bewahren und keine persönlichen Daten am Telefon preiszugeben. Im Zweifel nach der Telefonnummer fragen und einen Rückruf versprechen. So gewinnt man Zeit und kann die Telefonnummer des Anrufenden und die Echtheit des Anrufs überprüfen.

Aktuelle Warnung: Falsch angezeigte Telefonnummern / Spoofing

Beim „Spoofing“ (Englisch für „Fälschen“ oder „Vortäuschen“) versuchen Angreifer ebenfalls, eine vertrauenswürdige Kommunikation vorzutäuschen, um an persönliche Daten zu gelangen. Beim „Call-ID-Spoofing“ wird durch technische Manipulation auf dem Display eine andere Anrufer-Nummer angezeigt, als die von welcher der Anruf tatsächlich erfolgt. Damit wird ein „echter“ Anruf, beispielweise Ihrer Bank oder einer Behörde, vorgetäuscht.

Lassen Sie sich am Telefon nicht unter Druck setzen! Ihre Bank, die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Europol oder die Polizei wird Sie niemals telefonisch zur Herausgabe persönlicher Daten, wie zum Beispiel Bankkontodaten, drängen. Sie sollten das Gespräch beenden und anschließend die Bank und Polizei anrufen, um den Sachverhalt zu klären beziehungsweise anzuzeigen. Verwenden Sie dafür aber nicht die Rückrufunktion des Telefons, sondern wählen Sie die Ihnen bekannte Nummer manuell. Lassen Sie sich auch nicht auf Angebote zur Fernwartung Ihres Rechners wegen angeblicher Bedrohung oder technischer Probleme ein. Auch sollten Sie Aufforderungen zur Zahlung auf ein „sicheres“ Konto am Telefon nicht nachkommen.

Aktuelle Warnung: Gefälschte Nachrichten aus sozialen Medien

Wer sich in dem beruflichen Netzwerk angemeldet hat, kennt die regelmäßigen Nachrichten: „Sie wurden in so und so viel Suchen gefunden“ „Sie haben eine Kontaktanfrage oder Nachricht bekommen“. Auch diese Meldungen können täuschend echt nachgebildet sein mit dem Ziel, an persönliche Anmeldedaten zu kommen oder auf eine gefälschte Seite weiterzuleiten.

Erkennen kann man die betrügerischen Mails an kleinen Fehlern, z. B. „Linkedin“ statt „LinkedIn“, eine unübliche Absenderadresse oder Ungenauigkeiten in Text oder Logo. Klickt man den betrügerischen Link an, wird man auf eine Fake-Seite weitergeleitet, um auf diese Weise an persönliche Daten wie zum Beispiel die Telefonnummer zu gelangen. Ist diese in den Händen der Betrüger, wird versucht, mit gezielten Anrufen an weitere persönliche Daten zu gelangen.

Übertragen lassen sich diese Betrugsmaschen auf andere Social-Media-Kanäle: Ganz gleich, ob Facebook, Instagram, „X“ oder Nachrichten vom E-Mail-Dienstleister. Man sollte bei jeder Nachricht im Hinterkopf die Möglichkeit bedenken, dass es sich um einen Betrug handeln kann. Und gerade vor zu schnellen, unbedachten Klicks sollte man sich hüten.

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 nachzulesen.

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

Ferner 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 sowie 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.

M.M.WARBURG & CO
BANK

www.mmwarburg.de