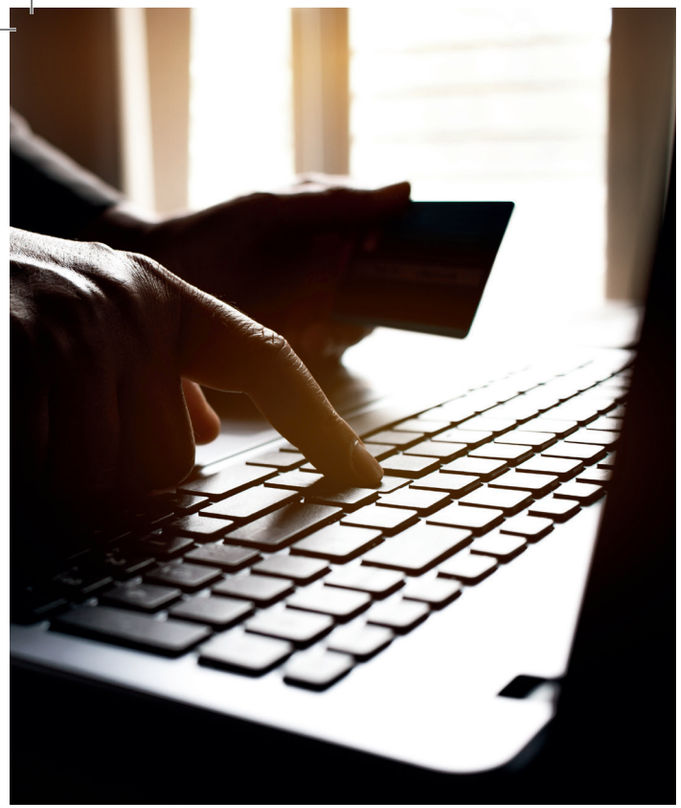


Weitere Informationen finden Sie unter:

Phishing | Smishing | Vishing – Watchlist Internet

Vorfälle können Sie per E-Mail melden:

against-cybercrime@bmi.gv.at

Dies ersetzt jedoch nicht die Anzeigeerstattung bei der Polizei.

PSA

KRIMINAL PRÄVENTION

Bundesministerium Inneres

Bundeskriminalamt

POLIZEI

Impressum
MedieninhaberIn, VerlegerIn und HerausgeberIn:
Bundeskriminalamt
Josef-Holaubek-Platz 1, 1090 Wien
+43 1 24836 985025
AutorInnen: Büro für Kriminalprävention und Opferhilfe, BMI I/C/10
Fotonachweis: Adobe Stock
Gestaltung: BMI I/C/10/a – Strategische Kommunikation und Kreation
Druck: Gerin Druck GmbH
Wien, 2024

www.kriminalpraevention.gv.at

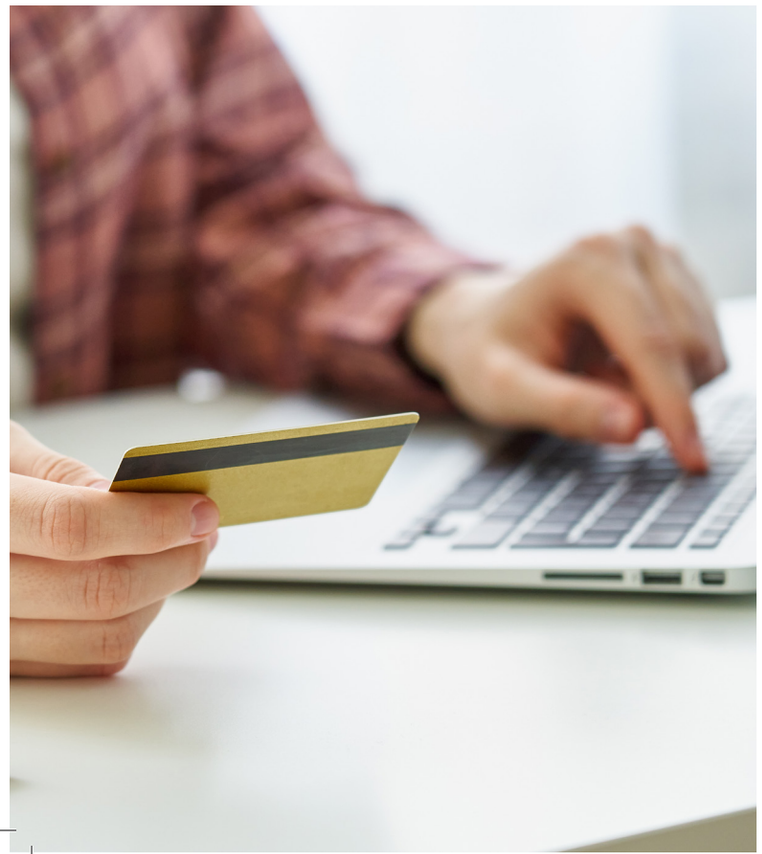
Anti-Phishing

Richtiges Vorgehen und Schutz vor Phishing



Was ist Phishing?

Cyber-Kriminelle kontaktieren Sie telefonisch oder verschicken betrügerische Nachrichten per E-Mail, SMS, über Messengerdienste oder soziale Netzwerke. In diesen ist ein Link oder Anhang enthalten, über den Sie aufgefordert werden, vertrauliche Informationen wie Zugangsdaten, Passwörter oder Kreditkartendaten preiszugeben. Die Nachrichten wirken oft täuschend echt und die Absender seriös. Daher schöpfen viele keinen Verdacht und geben Daten an Kriminelle weiter.



Richtiges Vorgehen nach Eingabe der Daten

- Wenn Sie auf einen dieser Links geklickt haben und Zahlungsdaten eingegeben haben, lassen Sie unverzüglich Ihre Online-Banking-Dienste bzw. Ihr Bankkonto und Ihre Karten sperren. Behalten Sie die Umsätze am Konto im Auge und kontaktieren Sie sofort Ihre Bank. Sammeln Sie alle Beweise wie die betrügerische E-Mail-Nachricht, SMS oder Whatsapp-Chats und geben Sie die Beweise erst nach Aufforderung von der Bank oder der Polizei weiter. Nach der Entsperrung Ihres Kontos ist es wichtig, ausschließlich neue Passwörter und PIN-Codes für Ihr Konto zu verwenden.

- Wenn Sie Ihre Zugangsdaten zu Konten von Online-Shops oder Ihrem E-Mail-Konto weitergegeben haben, ändern sie Ihr Passwort und nehmen Sie Kontakt mit dem Anbieter auf. Für verschiedene Online-Shop-Konten sollten Sie auch verschiedene Passwörter verwenden, um den Zugang für Kriminelle zu erschweren. Mit dem Zugang zu Ihrem E-Mail-Postfach können auch andere Online-Dienste kompromittiert sein. Auch hierbei ist die Änderung der Passwörter dringend notwendig. In diesem Fall können Zahlungsdaten ebenso betroffen sein, daher kontrollieren Sie Ihr Konto und Ihre Karten und kontaktieren Sie die Bank.

- Sollten die Betrüger Geld von Ihnen verlangen, gehen sie keinesfalls auf die Forderungen ein. Wenden Sie sich an die nächste Polizeidienststelle, bringen Sie alle vorhandenen Unterlagen mit und erstatten Sie eine Anzeige.

Schutz vor Phishing

- Die Aktualisierung der Computersoftware und des Betriebssystems sowie die Installation zusätzlicher Anti-Viren-Programme schützen vor möglichen Phishing-Attacken.

- Seien Sie skeptisch, wenn sie Nachrichten von unbekannten Absendern erhalten. Banken, Dienstleister oder Behörden werden Sie niemals per E-Mail, SMS oder Messengerdienst zur Herausgabe von Passwörtern auffordern. Im Zweifel suchen Sie sich die Telefonnummer des Absenders selbst heraus und lassen sich die Nachricht vom Absender telefonisch bestätigen. E-Mail-Anhänge in den Formaten „.exe“ oder „.scr“ können Schadsoftware enthalten, die beim Öffnen direkt auf das Gerät geladen wird. Durch Doppelendungen wie „.pdf.exe“ wird versucht, Sie in die Irre zu führen.

- Nach Möglichkeit verwenden Sie bei den Online-Shop- oder E-Mail-Konten die Zwei-Faktor-Authentifizierung, denn durch die zweite Stufe der Identifizierung können die Täter auch mit dem erlangten Passwort nicht auf Ihre Daten zugreifen.