POLIZEI
Nordrhein-Westfalen
Dortmund

Phishing & Identitätsdiebstahl

Quelle: adobe stocks (Polizei NRW)

Sensibler Datenklau

POLIZEI Nordrhein-Westfalen Dortmund

Durch die Digitalisierung und alltägliche Verwendung des Internets besitzt heutzutage jeder über wenigstens eine digitale Identität im World Wide Web.

Diese Identität kann alle Arten von Accounts und zahlungsrelevanten Informationen eines Nutzers im Internet umfassen, wie zum Beispiel Zugangsdaten in den Bereichen

- Kommunikation (E-Mail, Messenger-Apps)
- E-Commerce (Banking, Online-Stores, etc.)
- Kreditkartendaten
- E-Government (elektronische Anträge, Steuererklärung)
- Cloud-Computing (Firmenplattformen, Fotos, Daten, etc.)

Unter dem Begriff „Phishing“ versteht man den Versuch, durch gefälschte E-Mails (mit Schadcode im Anhang oder Link zu einer präparierten Website), gefälschte Webseiten, Kurznachrichten oder Videolinks an die persönlichen Daten eines Internetnutzers zu gelangen und so einen Identitätsdiebstahl zu begehen.

Durch Phishing, dem „Abfischen“ von sensiblen Daten wie Passwörtern, Adressdaten, Bankdaten, Pins, TANs, Kreditkarten- und Handynummern und Profildaten können Cyberkriminelle die Identität des Betroffenen übernehmen (Identitätsdiebstahl) und großen (finanziellen) Schaden verursachen.

Jeder Betroffene sollte sich direkt an die Polizei wenden!

Wie gehen die Täter vor?

POLIZEI
Nordrhein-Westfalen
Dortmund

Die Täter verwenden hier gefälschte, täuschend echt aussehende E-Mails und Links zu Websites von namenhaften Marken, Unternehmen, Händlern oder Banken um die Opfer zu ködern.
Geben die Betroffenen dann ihre persönlichen Daten, Passwörter etc. in die fingierten Eingabemasken ein, schicken sie diese dann unbewusst an die Cyberkriminellen.

Quelle: adobe stocks (Polizei NRW)

Mit diesen Daten können Täter dann beispielsweise persönliche Nachrichten mit Schadcode an die Bekannten/Freunde des Opfers verschicken, Onlinekäufe tätigen, die sensiblen Daten gewinnbringend weiter verkaufen oder weitere Straftaten im Namen des Geschädigten begehen.

Wie kann man sich schützen?

POLIZEI Nordrhein-Westfalen Dortmund

Starke Passwörter verwenden

Stark ist ein Passwort, wenn es aus mindestens neun Zeichen unter Nutzung von Klein- und Großbuchstaben, Ziffern und Sonderzeichen besteht. Bitte keine Namen, Geburtsdaten oder Passwörter aus dem Wörterbuch verwenden und auf keinen Fall an Dritte weiter geben. Es wird empfohlen, für verschiedene Onlinezugänge auch unterschiedliche Nutzernamen und Passwörter zu verwenden. Diese Passwörter sollten auch an geeigneten Stellen und vor Dritten geschützt aufbewahrt werden. Optimal ist auch die Verwendung eines Passwortmanagers mit Schlüsselbundfunktion.

Verwenden Sie keine Passwörter, die in der Vergangenheit schon einmal benutzt wurden und vermeiden Sie die „Passwort merken“-Funktion von Anwendungen im Browser und in Applikationen (Apps). Bevorzugt werden sollten auch Dienste, welche die Zwei-Faktor-Authentifizierung unterstützen.

Privatsphäre schützen

Richtige Sicherheitseinstellungen auf den Endgeräten sowie in den Sozialen Medien reduzieren das Risiko, zu viele Informationen von sich selbst preiszugeben. Ein sorgfältiger Umgang mit seinen Profildaten und Bildern ist unerlässlich.

=> Seien Sie sparsam mit der Weitergabe Ihrer persönlichen Daten!

[Profilbild, personenbezogene Daten, Freunde-Einstellungen, öffentliche-Daten, Selfies, Likes]

Misstrauisch sein

Bei Anfragen von Unbekannten immer misstrauisch sein! Cyberkriminelle verstecken sich in erster Linie hinter anonymen, gefälschten und unseriösen Profilen. Aus diesem Grund sollte jede Kontaktanfrage immer kritisch hinterfragt und keine sensiblen Daten herausgegeben werden. Auch E-Mails von Unbekannten sollten weder geöffnet, noch sollten Anhänge und Links in keinster Weise angeklickt werden. Hier verbirgt sich oftmals Schadsoftware, mit der Absicht Passwörter zu erbeuten, um weitere, kriminelle Handlungen durchzuführen. Oftmals lassen sich Betrüger auch durch die unkorrekte Schreibweise der E-Mailabsenderadresse, deren Inhalt, falsche Umlaute, kryptische Buchstaben oder anhand der Linkadresse erkennen. Eine sichere Website erkennt man am „**s**“ (secure) in der Kopfadresse bei http**s**://...

Wo gibt es Hilfe?

POLIZEI Nordrhein-Westfalen Dortmund

Wenn man Opfer von Cybercrime geworden ist, stehen einem die gleichen umfangreichen Hilfs- und Unterstützungsangebote zur Verfügung, wie den Opfern von Straftaten in der realen Welt.

Bei akuter Bedrohung, wählen Sie 110! Die Polizei wird alles Erforderliche tun, um Sie zu schützen.

- Zeigen Sie die Straftat bei der Polizei an (Strafanzeige ist bei jeder Polizeidienststelle möglich)
- Existierendes Datenmaterial, wie z. B. E-Mails, Chat-Verläufe in Messenger-Diensten, digitale Fotos oder Videos sind wichtige Beweismittel, die Sie bis zum ersten Kontakt mit der Polizei bestenfalls komplett unverändert lassen.
- Bringen Sie das gesicherte Beweismaterial am besten gleich zur Anzeigenerstattung mit. Das ist wichtig für die weiteren Ermittlungen, um den Verlust von Spuren im Netz zu vermeiden.