Warnung der Polizei im Weserbergland und in Südniedersachsen

Hände weg von der E-Mail-Info: "Paket in der Warteschleife"

Donnerstag 29. September 2022 - **Hameln** / **Holzminden** / **Göttingen (wbn). Die Polizei im Weserbergland warnt aus gegebenem Anlass vor E-Mail-Betrügern im Internet. Aktuell wird Missbrauch betrieben mit der Behauptung "Paket in der Warteschleife". Damit sollen ganz persönliche sensible Angaben "abgefischt" werden**
.

Nachfolgend die Warnung der Polizei im Wortlaut: "Die Polizei warnt vor betrügerischen E-Mails. Die Täter versenden fingierte E-Mails, so genannte Phishing-Mails, oder treten in sozialen Netzwerken als vertrauenswürdige Person auf.

Fortsetzung von Seite 1 Sie wollen Empfänger dazu veranlassen, persönliche Daten wie Zugangsdaten, Passwörter, Transaktionsnummern usw. preiszugeben. Internetbetrüger ködern ihre Opfer mit fingierten E-Mails und führen sie auf professionell gestaltete Internetseiten. Dort sollen sie ihre Zugangsdaten eingeben. Aktuell fordert eine DHL-Phishing-Mail zur Bezahlung von Versandgebühren auf.

Aufgepasst bei der Nachricht "Paket in der Warteschleife"! Angeblich wurde die Versandgebühr noch nicht bezahlt, weshalb das Paket noch nicht zugestellt werden konnte. Über einen beigefügten Link könne man es nachhohlen und den Versand bestätigen.

Auch, wenn die Mail auf den ersten Blick seriös erscheint: Es handelt sich um einen Betrugsversuch!

Mit den abgefischten persönlichen Daten können Betrüger Missbrauch betreiben ("Identity Theft" = Übernahme einer fremden Identität) und mit der vorgegaukelten Identität im Namen des Geschädigten online nahezu alle Geschäfte abwickeln (Geld überweisen, Dispokredit ausschöpfen, Online-Einkäufe tätigen etc.). So entsteht Jahr für Jahr ein beträchtlicher wirtschaftlicher Schaden.

Allgemeine Tipps zum Schutz vor Phishing - Beachten Sie: Kreditkarteninstitute werden solche Schreiben niemals versenden und Sie zur Eingabe persönlicher Daten im Internet auffordern - auch nicht, um der Sicherheit willen. - Vergewissern Sie sich, mit wem Sie es zu tun haben. Überprüfen Sie die Adressleiste in Ihrem Browser.

Bei geringsten Abweichungen sollten Sie stutzig werden. Tragen Sie ständig benötigte Internet-Adressen in die Favoritenliste Ihres Browsers. - Klicken Sie niemals auf den angegeben Link in der übersandten E-Mail. Versuchen Sie stattdessen, die in der E-Mail angegebenen Seiten über die Startseite Ihrer Bank zu erreichen (ohne diese in die Adresszeile einzutippen). - Kreditinstitute fordern grundsätzlich keine vertraulichen Daten per E-Mail oder per Telefon oder per Post von Ihnen an. Wenn Sie sich unsicher sind, halten Sie in jedem Fall Rücksprache mit Ihrer Bank. - Übermitteln Sie keine persönlichen oder vertraulichen Daten (bspw. Passwörter oder Transaktionsnummern) per E-Mail. - Folgen Sie Aufforderungen in E-Mails, Programme herunterzuladen, nur dann, wenn Sie die entsprechende Datei auch auf der Internet-Seite des Unternehmens finden (Starten Sie keinen Download über den direkten Link). Öffnen Sie insbesondere keine angehängten Dateien. Nutzen Sie Antivirenprogramme und Firewalls. - Geben Sie persönliche Daten nur bei gewohntem Ablauf innerhalb der Online-Banking-Anwendung Ihres Kreditinstituts an. Sollte Ihnen etwas merkwürdig vorkommen, beenden Sie die Verbindung und kontaktieren Sie Ihre Bank. - Beenden Sie die Online-Sitzung bei Ihrer Bank, indem Sie sich abmelden.

Schließen Sie nicht lediglich das Browserfenster und wechseln Sie vor Ihrer Abmeldung nicht auf eine andere Internetseite. - Kontrollieren Sie regelmäßig Ihren Kontostand sowie Ihre Kontobewegungen.

So können Sie schnell reagieren, falls ungewollte Aktionen stattgefunden haben. - PIN und TANs sollten Sie nur dann eingeben, wenn eine gesicherte Verbindung mit Ihrem Browser hergestellt ist. Eine Sichere Verbindung erkennen Sie an dem https:// in der Adresszeile: Im Browserfenster erscheint ein kleines Icon, z. B. in Form eines Vorhängeschlosses, das den jeweiligen Sicherheitsstatus symbolisiert ("geschlossen" bzw. "geöffnet"). - Nutzen Sie nur die offizielle Zugangssoftware Ihrer Bank. - Nutzen Sie Funktastaturen nur dann für das Online-Banking, wenn diese über eine eingebaute Verschlüsselung verfügen.

Dies gilt auch für die Nutzung von Wireless-LAN (WLAN). - Achten Sie auf einen Grundschutz Ihrer Hard- und Software. Weitere Informationen dazu finden Sie im Sicherheitskompass von Polizei und BSI."