POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

bürgerorientiert · professionell · rechtsstaatlich

Betrugsversuche im Zusammenhang mit dem Corona-Virus („Phishing“)

In der aktuellen Corona-Pandemie nutzen Straftäter Angst und Unsicherheit in der Bevölkerung aus, um sich skrupellos zu Lasten ihrer Opfer zu bereichern. Die Täterinnen und Täter setzen dabei insbesondere auf die Möglichkeiten des Internets.

Phishing-E-Mails

Die Täter behaupten, als Dienstleister im Online-Sektor, zum Beispiel Banken und Sparkassen, nur per Telefon oder E-Mail weiterhelfen zu können. Die Kundinnen und Kunden werden per E-Mail aufgefordert, ihre Daten abzugleichen, insbesondere Passwörter oder andere sensible Daten auf Web-Seiten einzugeben, die täuschend echt aussehen. Tatsächlich werden die Daten auf eine betrügerische Seite eingegeben und die Täterinnen und Täter gelangen so in den Besitz aller nötigen Angaben, um diese wiederrum für weitere Tathandlungen nutzen zu können. Diese E-Mails emotionalisieren und greifen die Empfehlungen auf, sich nicht unnötig im Freien aufzuhalten.

Phishing-E-Mails erkennen

Gemeinsam mit der Verbraucherzentrale Nordrhein-Westfalen empfiehlt die Polizei Nordrhein-Westfalen folgendes:

Es gibt nach wie vor ein paar typische Merkmale, an denen Sie eine Phishing-E-Mail erkennen können:

Sind Sie Kunde bei der genannten Bank oder dem Unternehmen? Wenn nicht, ist es ein ziemlich eindeutiger Hinweis auf Betrug!

Der Absender der E-Mail nutzt keine Internet-Adresse der Firma, die in der Nachricht als Absender genannt wird. Zwar lässt sich leicht fälschen, was als Absender angezeigt wird, aber Sie können im sogenannten Header prüfen, von wem die E-Mail tatsächlich stammt.

Die Anrede ist oft unpersönlich. Allerdings gibt es auch zahlreiche Beispiele, in denen Sie von Betrügern mit Ihrem richtigen Namen angesprochen werden. Deshalb sollten Sie auch bei richtiger persönlicher Anrede noch misstrauisch sein!

Enthaltene Links führen auf eine gefälschte Internetseite. Prüfen Sie **vor** dem Anklicken unbedingt das „Linkziel“! Lesen Sie die Internetadresse genau! Manchmal verändern die Betrüger nur Kleinigkeiten. Am besten klicken Sie keinen Link in einer E-Mail an, sondern öffnen die Ihnen bekannte echte Seite Ihrer Bank in einem Browser.

Stand: März 2020

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 ein.
- 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, 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 https://www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/sicherheitskompass/

Was muss ich beachten, wenn ich Opfer geworden bin?

Erstatten Sie immer Strafanzeige! Beachten Sie bitte zurzeit die mögliche Vermeidung von persönlichen Kontakten und wählen Sie den fernmündlichen Kontakt zur Polizei oder nutzen Sie die Möglichkeit, eine Strafanzeige auch Online zu erstatten https://polizei.nrw/internetwache.

Weiterführende Hinweise und Links

www.polizei-beratung.de

www.bsi.bund.de

www.verbraucherzentrale.de

Herausgeber
Landeskriminalamt Nordrhein-Westfalen
Abteilung 3, Dezernat 32
Völklinger Str. 49
40221 Düsseldorf

Stand: März 2020