Bundesministerium
Inneres

Bundeskriminalamt

bundeskriminalamt.at

II/BK/Abteilung 5/ Büro 5.2 –
C4, Cybercrime Competence Center
c4-meldestelle@bmi.gv.at

Tel: +43 1 24836-986500

Josef-Holaubek-Platz 1, 1090 Wien

E-Mail-Antworten sind bitte unter Anführung der Geschäftszahl an c4-meldestelle@bmi.gv.at zu richten.

Sehr geehrte Damen und Herren!

Aufgrund der derzeitigen Corona-Krise möchten wir Sie auf folgendes aufmerksam machen:

**Die aktuelle Situation führt bei vielen Menschen verständlicherweise zu Verunsicherung. Kriminelle nutzen häufig derartige Situationen aus, um sich zu bereichern!**

Sie werden daher in der nächsten Zeit, insbesondere auch im digitalen Bereich verstärkt damit rechnen müssen, dass Kriminelle unter dem Deckmantel „Corona" es versuchen, Ihnen einen Schaden zuzufügen.

Das könnte zum Beispiel wie folgt passieren:

- eine Webseite fordert Sie auf, ihre Daten einzugeben, um über die aktuellsten Entwicklungen im Zusammenhang mit Corona informiert zu bleiben.
- eine Mail fordert Sie auf, eine neue Software für die Telearbeit zu installieren.
- eine Mail fordert Sie auf, Ihr Passwort auf einer Webseite einzugeben, um das neue Zusammenarbeitstool (Videokonferenzen, Chattools, ...) zu aktivieren.
- ein Popup-Fenster erscheint auf Ihrem Bildschirm, in dem Sie das „Sicherheitsteam" auffordert, die Installation und Freigabe eines erforderlichen Remote-Tools zu akzeptieren.

Daher bitten wir Sie um Beachtung folgender Sicherheitsgrundsätze:

- Seien Sie skeptisch, wenn Sie z.B. per E-Mail zu ungewöhnlichen oder auch scheinbar notwendigen Handlungen aufgefordert werden oder auf Seiten verwiesen werden, auf der Sie ein Passwort oder persönliche Daten eingeben sollen. Bedenken Sie, dass die **Absenderadresse oder der Name in solchen E-Mails gefälscht sein könnten**.

- Prüfen Sie die Korrektheit: Grundlegende Änderungen von Prozessen in einer Organisation werden auf deren Homepage, in Team-Sitzungen oder durch interne Verlautbarungen bekannt gemacht. Falls Sie unsicher sind, fragen Sie bei der zuständigen Stelle nach. Scheuen Sie sich nicht, bei der zuständigen Stelle telefonisch nachzufragen, hier können die meisten „Unklarheiten" geklärt werden.

- Geben Sie Zugangsdaten nur auf Webseiten ein, bei denen die Adresse [der erwartete Domainname] unmittelbar vor dem ersten Schrägstrich steht. Wenn Sie sich unsicher sind, geben Sie die Web-Adresse händisch ein, damit verhindern Sie zumeist, dass Sie auf einer sog. „Fake-Seite" landen (z.B. Coce-lola.xx anstatt von Coca-lola.xx).

- „Sichere" Webseiten werden zumeist durch das Präfix https angezeigt:

  https://stp.portal.bka.gv.at/

  Leider ist in diesem Zusammenhang zu erwähnen, dass durch Organisationen die Verwendung von „https:" (nahezu) kostenlos zur Verfügung gestellt wird. Wenn Sie einen „anerkannten" Web-Browser verwenden, wird Sie dieser in der Informationsleiste darüber informieren, ob es sich um eine „sichere" Seite handelt" (grünes Schloß, Haken, etc.).

  **Beispiel einer unsicheren Adresse:**

  https://webhoster-a.com/stp.portal.bka.gv.at (Anderer Domänenname vor dem ersten Schrägstrich)

  https://bka.gv.at@irgendetwasanderes.com/ (Vor dem ersten Schrägstrich befindet sich „irgendetwasanderes.com", nicht „bka.gv.at")

- Beachten Sie bitte unbedingt die Schreibweise von Ihnen übermittelten Web-Adressen. Wenn es sich um Ihnen „bekannte Adressen" handelt, geben Sie diese unbedingt händisch oder aus Ihren Aufzeichnungen mittels copy/paste ein. Übernehmen Sie im Zweifelsfall keineswegs Web-Links, welche Ihnen per E-Mail übermittelt wurden.

- Weder ein Kreditinstitut noch eine namhafte Vertretung eines Geschäftspartners, wird Sie jemals per Mail oder Popup auffordern, auf einen Link zu klicken oder persönliche Angaben zu bestätigen, keines Falles eine Ausweis-Kopie zu übermitteln.

- Wenn Sie E-Mails von Firmen, Bekannten und Freunden erhalten, sehen Sie sich bitte immer die ganze Emailadresse an und achten Sie insbesondere darauf, dass der Namens-

Teil als auch die angeführte Domäne hinter dem @ jenem Mail-Anbieter entspricht, der Ihnen dazu bekannt ist. Oftmals werden von Tätern gleichlautende Mail-Adressen unter Verwendung unterschiedlicher Domänen verwendet.

- Haben Sie Ihre Zugangsdaten auf einer vermeintlich unsicheren Webseite eingegeben, ändern Sie sofort das Passwort und informieren Sie die für Sie zuständige IT-Abteilung, um allfällige missbräuchliche Zugriffe in diesem Zeitraum zu dokumentieren und festzuhalten.

Sollten Sie in diesem Zusammenhang nicht erklärliche oder nicht nachvollziehbar E-Mails erhalten, können Sie sich auch gerne, zwecks Abklärung an die C4-Meldestelle unter

**against-cybercrime@bmi.gv.at**

wenden. Fachkundige Beamte werden sich der Sache annehmen und versuchen, den vorliegenden Sachverhalt zu bewerten und Ihnen geeignete Schritte empfehlen.

Wien, 13. März 2020