Bundesministerium
Kunst, Kultur,
öffentlicher Dienst und Sport

bmkoes.gv.at

An alle Mitarbeiterinnen und Mitarbeiter

im Bundesministerium für Kunst, Kultur, öffentlichen Dienst und Sport

Corona-Virus (COVID-19)

Cybersecurity

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. Genau das wird von Cyberkriminellen ausgenutzt.

Sie werden daher in der nächsten Zeit verstärkt damit rechnen müssen, dass Kriminelle unter dem Deckmantel „Corona“ versuchen, an Ihre Passwörter zu kommen oder Schadsoftware auf Ihrem Rechner zu installieren.

Das könnte zum Beispiel wie folgt passieren:

- Eine Website fordert Sie auf, Ihre Daten einzugeben, um über die aktuellsten Entwicklungen im Zusammenhang mit Corona informiert zu bleiben.
- Eine E-Mail fordert Sie auf, eine neue Software für die Telearbeit zu installieren.
- Eine E-Mail fordert Sie auf, Ihr Passwort auf einer Website einzugeben, um das neue Zusammenarbeitstool (Videokonferenzen, Chattools, …) zu aktivieren.
- Ein Popup-Fenster erscheint auf Ihrem Bildschirm, in dem Sie das „Sicherheitsteam“ auffordert, auf einen Link zu klicken.

Daher bitte 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 eingeben sollen. Bedenken Sie, dass **Absenderadresse oder der Name in E-Mails gefälscht sein können**.
- Prüfen Sie die Richtigkeit: Grundlegende Änderungen von Prozessen in einer Organisation werden auf deren Homepage bekannt gemacht. Falls Sie unsicher sind, fragen Sie bei der zuständigen Stelle nach. Sie können auch bei einer Suchmaschine mittels Stichworten nachsehen: verbreitete Betrugsmaschen sind vielfach schon bekannt und dokumentiert.
- Geben Sie Ihr Passwort nur auf Webseiten ein, bei denen die Adresse [der erwartete Domainname] unmittelbar vor dem ersten Schrägstrich steht.
  Sicher:
  https://stp.bmg.gv.at/
  Unsicher:
  https://webhoster-a.com/stp.bmg.gv.at (anderer Domänenname vor dem ersten Schrägstrich)
  https://bmkoes.gv.at@irgendetwasanderes.com/ (vor dem ersten Schrägstrich befindet sich „irgendetwasanderes.com“, nicht „bmkoes.gv.at“)
- Das Sicherheitsteam wird Sie niemals per E-Mail oder Popup auffordern, auf einen Link zu klicken. Wenn Sie Rückfragen haben, kontaktieren Sie Ihren Ansprechpartner aus einer unabhängigen, sicheren Quelle (z.B. der Website) und verwenden Sie keine Ansprechpartner, die direkt in der Nachricht genannt werden, deren Echtheit Sie prüfen möchten.
  Sehen Sie sich immer die ganze E-Mail-Adresse an und achten Sie darauf, dass der Teil hinter dem @ der Domain entspricht, von der Sie die Nachricht erwarten (also z.B. @bmkoes.gv.at)

Sollten Sie Ihr Passwort auf einer unsicheren Website eingegeben haben, informieren Sie unmittelbar den Security Verantwortlichen, **Christopher Ozvald**, unter der Telefonnummer: **+43 71606 644131** oder per E-Mail: **christopher.ozvald@bmkoes.gv.at** und ändern Sie das Passwort.

In diesem Sinne wünschen wir Ihnen alles Gute. Das Team der IT steht Ihnen auch in dieser herausfordernden Zeit unterstützend zur Seite.

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2020-04-27T12:15:42+02:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel
Hinweis	Dieses Dokument wurde elektronisch besiegelt.	