

19. Dezember 2024 / Medienmitteilung

Achtung vor Betrugsversuchen!

Es kommt in letzter Zeit immer häufiger vor, dass die Mitarbeitenden der Stadt Buchs von Betrügerinnen und Betrügern auf ihre geschäftliche E-Mail-Adresse kontaktiert werden. Auch im privaten Umfeld werden die Betrugsversuche immer perfider und die Täterinnen und Täter greifen immer tiefer in die Trickkiste. Bleiben Sie aufmerksam!

Bei den Betrugsversuchen geben sich die Täterinnen und Täter beispielsweise als Behördenmitglieder oder andere vertrauenswürdige Personen aus, um durch geschickte Täuschung sensible Informationen oder finanzielle Vorteile zu erlangen.

Aktuelle Beispiele:

- E-Mail eines angeblichen Arbeitskollegen oder einer angeblichen Arbeitskollegin mit der Aufforderung eine dringende Aufgabe zu erledigen, welche beispielsweise den Kauf von Gutscheinen beinhaltet und die Gutschein-Codes per E-Mail zugestellt werden sollen.
- Anruf eines angeblichen Dienstleisters, um eine ausstehende Rechnung, ein Computer-Problem oder ähnliches via Online-Zahlung direkt aus dem Weg zu schaffen oder dabei Ihre Zugangsdaten zu erfahren.
- Nachricht einer angeblich verwandten Person in dringender Not und mit dem Ziel Geld via Überweisung zu erlangen.
- Hinweis via SMS oder E-Mail, dass Ihr Paket nicht zugestellt werden konnte oder dies noch abgeholt werden muss mit dem Ziel an Ihre Zugangsdaten zu gelangen.

So können Sie Betrugsversuche erkennen:

- Druck durch angebliche Dringlichkeit: Es wird oftmals dringend um Hilfe gebeten, oft verbunden mit einer emotionalen Geschichte oder der klaren Aufforderung «sofort zu handeln».
- Betrugsversuche via E-Mail: Die Absenderadresse wirkt auf den ersten Blick echt, entspricht jedoch nicht einer offiziellen Mailadresse.
- Betrugsversuche via Messenger (WhatsApp & Co.): Die Nachrichten stammen von einer Nummer, welche nicht in Ihren Kontakten gespeichert ist. Es wird oftmals vorgegeben, dass die Person ihr Smartphone verloren hat oder dieses gestohlen wurde und sie daher via einer Ihnen unbekanntem Nummer kontaktiert werden.
- Ungewöhnliche Aufträge oder Aufforderungen: Nach dem Ihr Vertrauen gewonnen wurde, werden Sie aufgefordert, Gutscheine zu kaufen, Geld zu überweisen oder sensible Daten (z.B. Zugangsdaten) preiszugeben.

Unsere Empfehlungen:

- **Seien Sie skeptisch:** Überprüfen Sie die Absenderadresse sorgfältig. Offizielle E-Mails der Stadtverwaltung Buchs enden beispielsweise stets mit «@buchs-sg.ch» oder die der Schule Buchs mit «@schulebuchs.ch».
- **Kontaktieren Sie die angebliche Absenderin oder den Absender persönlich:** Nutzen Sie hierfür andere Möglichkeiten in Kontakt zu treten. Beispielsweise finden Sie unsere offiziellen Telefonnummern und unsere E-Mail-Adressen auf unserer Webseite unter www.buchs-sg.ch bzw. www.schulebuchs.ch.

- **Geben Sie keine sensiblen Informationen preis:** Übermitteln Sie niemals Zugangsdaten, Passwörter, Zahlungsinformationen per E-Mail, Messenger oder telefonisch.
- **Hinterfragen Sie die Aufforderung:** Behörden oder offizielle Institutionen würden niemals um den Kauf von Gutscheinen oder um die Angaben Ihrer Kreditkarte bitten.
- **Melden Sie Gefahren im Internet und Telefonbetrug:** Die Webseite des Kantons St. Gallen verweist unter «Häufig gestellte Fragen» zum Thema Cybercrime auf die Möglichkeiten, wie Sie diese melden können und vermittelt weiterführende Informationen zum Thema. Scannen Sie hierzu den QR-Code:



Gemeinsam gegen Betrug!

Ihre Aufmerksamkeit und Vorsicht sind der beste Schutz vor Betrügerinnen und Betrügern. Helfen Sie mit, unsere Gemeinschaft zu sensibilisieren, indem Sie diese Informationen auch mit Ihrem Umfeld teilen und das Thema «Online-Betrug» offen thematisieren.

Öffentliche Sicherheit der Stadtverwaltung Buchs

Kontakte

Medienkontakt:

Matthias Kramer, Kommunikationsverantwortlicher, 081 755 74 08, matthias.kramer@buchs-sg.ch