Erste-Hilfe bei Cybervorfällen

Sind Sie auf einen Betrug hereingefallen? Bleiben Sie ruhig und handeln Sie schnell.

Cyberkriminelle werden immer schneller und raffinierter. Dank KI klingen ihre gefälschten Stimmen, Videos und Texte heute täuschend echt – und machen Betrugsversuche schwerer erkennbar als je zuvor. Sie spielen mit unseren Emotionen: Angst, Dringlichkeit, Neugier oder sogar dem Wunsch, jemandem zu helfen. Ob es sich um eine Nachricht von einem „Kollegen", einen Anruf von Ihrer „Bank" oder ein Video Ihrer „Chefin" handelt, die um Hilfe bittet –es ist einfach in die Falle zu tappen. Aber selbst wenn Sie darauf hereingefallen sind, können Sie die Kontrolle noch zurückgewinnen.

Wie funktioniert's?

Betrüger nutzen unser Vertrauen – und unsern vollen Alltag. Mit KI-Tools können sie nun überzeugende Nachrichten, geklonte Stimmen und Deepfake-Videos erstellen. Diese scheinen oft von jemandem zu stammen, den Sie kennen oder dem Sie vertrauen. So läuft es in der Regel ab:

1. Sie erhalten eine Nachricht per E-Mail, Telefon, SMS oder über Messaging-Apps, in der Sie zu einer schnellen Handlung aufgefordert werden (eine dringende Zahlung oder ein Download).

2. Ihre Aufmerksamkeit ist geteilt, Sie sind gestresst oder emotional aufgewühlt – da ist es leicht Warnzeichen zu übersehen.

3. Die Situation wirkt glaubwürdig und dringend – und Sie handeln, ohne innezuhalten.

Sie sind nicht schuld – Betrüger nutzen Ihren Stress und Unaufmerksamkeit aus. Aber sobald Sie sich dessen bewusst sind, können Sie besser reagieren.

Erkennen Sie die Anzeichen

- Kenne ich diese Person wirklich? Oder ist es nur jemand, der einen bekannten Namen oder eine bekannte Nummer verwendet?
- Gibt es Links? Insbesondere verdächtige oder verkürzte URLs?
- Ist die Nachricht dringend oder bedrohlich? Zum Beispiel „Ihr Konto wird gelöscht“ oder „Ihr Freund ist in Gefahr“?
- Fühlt sich etwas seltsam an? Ungewöhnlicher Tonfall, unerwartete Anfragen?
- Werden sensible Daten oder Geld verlangt? Auch wenn es offiziell klingt?

Wenn einer dieser Punkte bei Ihnen Alarmglocken läuten lässt, handeln Sie nicht sofort. Stattdessen:

- Sprechen Sie mit jemandem, dem Sie vertrauen.
- Melden Sie den Vorfall gemäss den internen Verfahren Ihrer Organisation.
- Löschen Sie die Nachricht oder blockieren Sie den Absender.
- Interagieren Sie nicht weiter.

Was können Sie tun?

Erstens: **Keine Panik und keine Scham.** Diese Betrugsmaschen sind so konzipiert, dass selbst Expert:innen darauf hereinfallen. Entscheidend ist, wie Sie sich verhalten.

Wenn es im Privatleben passiert:

- Informieren Sie sofort Ihre Bank, wenn Geld oder Kartendaten betroffen sind. Wenn Sie betrogen wurden, erstatten Sie Anzeige bei der Polizei.
- Ändern Sie Ihre Passwörter und aktivieren Sie die Zwei-Faktor-Authentifizierung (2FA) für Ihre Konten.
- Führen Sie einen Malware-Scan auf Ihrem Gerät durch.
- Wenn Ihr Social-Media-Konto gehackt wurde, informieren Sie Ihre Kontakte, da diese möglicherweise Nachrichten von Ihrem gehackten Konto mit betrügerischen Links erhalten.
- Melden Sie den Vorfall Ihrer nationalen Stelle für Cyberkriminalität.
- Teilen Sie Ihre Erfahrungen mit Freunden und Familie. Ihre Geschichte kann anderen helfen, sich besser zu schützen.

Wenn es bei der Arbeit passiert:

- Melden Sie den Vorfall unverzüglich Ihrem IT- oder Sicherheitsteam. Je früher diese informiert sind, desto besser können sie helfen.
- Löschen Sie nichts, es sei denn, Sie werden dazu aufgefordert.
- Trennen Sie die Verbindung zum Netzwerk, wenn Sie sich bezüglich einer geöffneten Datei oder eines Links unsicher sind.
- Warnen Sie Ihre Kollegen, wenn sie ebenfalls betroffen sein könnten.

Be mindful. Stay safe.

Sie müssen keine Sicherheitsexpertin sein, um sich zu schützen. Nehmen Sie sich einfach einen Moment Zeit, bevor Sie klicken, reagieren oder antworten.

Wenn Ihnen etwas seltsam vorkommt, ist es wahrscheinlich auch so. Und wenn Ihnen ein Fehler unterlaufen ist: Bleiben Sie ruhig.
Eine schnelle Reaktion kann entscheidend sein.

Erfahren Sie mehr

🔗Erste Hilfe bei Cyber-Unfall: Was tun, wenn's passiert?
(Quelle: iBarry)
🔗 Responding to a cyber incident – a guide for CEOs (source: NCSC UK)

GÉANT