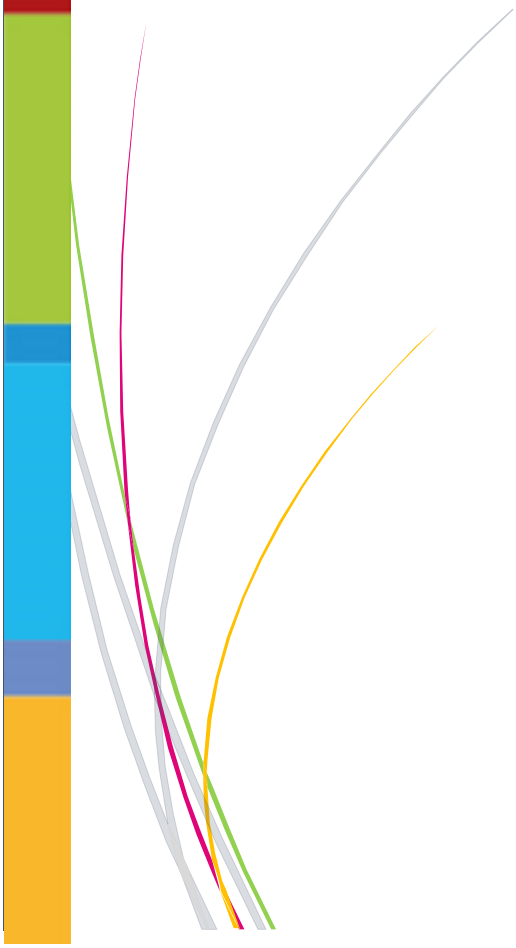
5.12.2024

Digitale Betrugsmethoden



Autor: DMS
AGH DIGITALES

Erbschleicher*innen

Kontaktaufnahme:
Meist über Telefon, seltener über Nachricht via SMS oder Messenger Diensten

Information

Schenkung, Vollmacht, Testament

Die Betrüger*innen versuchen Sie zu täuschen, einzuschüchtern und zu manipulieren, um Ihren letzten Willen zu beeinflussen. Bei der Täuschung wird der Erblasser*innen über die wahre Identität der Anrufenden getäuscht. Durch Einschüchterung sowie Drohungen wird Druck ausgeübt, um Erblasser*innen zu zwingen, das Erbe zu überlassen. Erbschleicher*innen manipulieren sowie Gefühle als auch den Zustand des*r Erblassers*innen um das Vertrauen zu gewinnen.

Prävention

- Ein verdächtiges Verhalten kann zum Beispiel eine schnellere emotionale Annäherung von Erbschleicher*innen und weitreichende Fokussierung auf Erblasser*innen sein.
- Achten Sie darauf, ob die Person beabsichtigt, Ihre Meinung bezüglich Ihres Testaments zu beeinflussen, indem Misstrauen gegenüber anderen geschürt wird.
- Als Erblasser*innen sprechen Sie besser offen mit der Familie und warten Sie die Reaktionen ab.

Was tun, wenn Sie Opfer geworden sind?

- Besorgen Sie sich anwaltliche Hilfe im Falle einer außerfamiliäreren Person.
- Erbunwürdigkeit abklären.
- Lassen Sie sich, bevor das Testament angefertigt wird, beraten.

Falsche Bankangestellte

Kontaktaufnahme:

Meist über Telefon, seltener über E-Mail, Nachricht via SMS oder Messenger Diensten

Information

Die Täter*innen erwecken bei ihrer Kontaktaufnahme den Eindruck, dass sie von der Bank stammen. Diese Nachrichten erhalten dann oft alarmierende Behauptungen, etwa, dass eine große Transaktion oder verdächtige Aktivitäten auf Ihrem Konto stattgefunden haben sollen. Durch Panikmache sollen Sie dann Betrüger*innen Passwort, PIN, TAN oder andere vertrauliche Daten geben. Manchmal wird auch eine Überweisung auf ein „sicheres“ Konto angefordert.

Prävention

- Verifizierung der Identität: Rufen Sie Ihre Bank an. Die Nummer finden sie auf der offiziellen Website oder in Ihren eigenen Bankunterlagen.
- Ihre Bank wird Sie niemals nach vertraulichen Daten wie Passwörter, PINs, TANs fragen. Insbesondere nicht via E-Mail, SMS oder Telefon.
- Lassen Sie sich nicht verängstigen, überrumpeln oder durch Druck dazu bewegen, den Bitten von Betrüger*innen nachzukommen.

Was tun, wenn Sie Opfer geworden sind?

- Rufen Sie direkt bei der Polizei an, ggf. in Kooperation mit Ihrer Bank.
- Rufen Sie die Bank an, um Ihr Konto sperren zu lassen.

Falsche Handwerker

Kontaktaufnahme:
Meist über Telefon, direkt an der Haustür, seltener über E-Mail und Post

Information

Dringliche Baumaßnahmen (z.B. Wasserschäden, Renovierungs-maßnahmen)

Die Betrüger*innen erzählen Ihnen, dass es durch Bauarbeiten im Haus oder in der Nachbarschaft zu Wasserschäden oder Verunreinigungen des Trinkwassers gekommen ist. Die Täter*innen betonen, dass es dringend sei und es deswegen vorab keine Benachrichtigung per Post/Email gegeben hat.

Prävention

- Öffnen Sie Ihre Tür nur mit vorgelegter Kette, alternativ schauen Sie durch den Türspion oder benutzen Sie die Türsprechanlage.
- Lassen Sie grundsätzlich keine Unbekannten in Ihre Wohnung/Haus.
- Lassen Sie Tür zu und rufen Sie die Polizei.
- Lassen Sie sich den Firmen Namen geben und überprüfen Sie deren Seriosität.
- Geben Sie niemals Geld an unbekannte Personen.
- Vorsicht bei Vertretergesprächen via Telefon

Was tun, wenn Sie Opfer geworden sind?

- Rufen Sie direkt bei der Polizei an und lassen Betrüger*innen draußen warten. Notieren Sie ggf. das Kfz Kennzeichen der Betrüger*innen.
- Beim kleinsten Verdacht Polizei kontaktieren, versuchen Sie den Betrüger*innen Daten herauszulocken.
- Rufen Sie Hilfe von umliegenden Nachbarn.

Falsche Polizisten

Kontaktaufnahme:
Meist über Telefon, direkt vor der Haustüre, eher selten über Post oder E-Mail

Information

Polizei, Europol oder sogar Interpol

Die Täter*innen rufen per Telefon an und schildern zum Beispiel, dass eine Einbruchsbande festgenommen wurde, bei denen eine Liste möglicher Einbruchopfer gefunden wurden. Im Anschluss werden Sie aufgefordert Ihre Wertsachen und Bargeld einem „Kollegen*innen“ zu geben. Anschließend werden Sie unter Druck gesetzt, dass Sie sich nicht weigern können, etwa, dass Sie „verpflichtet“ sind zu helfen, um die „Täter*innen“ festnehmen zu können.

Prävention

- Lassen Sie grundsätzlich keine Unbekannten in Ihre Wohnung/Haus.
- Lassen Sie sich am Telefon nicht unter Druck setzen.
- Geben Sie niemals Geld/Wertsachen an unbekannte Personen.
- Geben Sie niemals ihre Bankkarte/Bankdaten heraus und verraten Sie niemandem Ihre PIN.
- Prüfen sie, ob der „Polizist*innen“ im Besitz eines Dienstausweises ist, prüfen sie diesen auf Richtigkeit.
- Beim kleinsten Verdacht Polizei kontaktieren.
- Versuchen Sie dem Betrüger*innen Daten herauszulocken.

Was tun, wenn Sie Opfer geworden sind?

- Rufen Sie direkt bei der Polizei an und machen Sie Betrüger*innen nicht die Tür auf.
- Machen Sie Mitschriften zum Telefonat, sichern Sie Beweismittel.

Kaffeefahrt/Butterfahrt

Kontaktaufnahme:
Briefkästen mit falschen Angeboten und personenbezogene Werbemails und Anrufe

Information

Günstiges Ausflugsangebot?

Viele Reiseunternehmen bieten Kaffeefahrten zu schönen Orten an.
Wenn Sie auf einer unseriösen Kaffeefahrt sind, wird der versprochene Ort oft nicht angesteuert. Stattdessen werden Sie in eine Verkaufsveranstaltung gesetzt, in welcher Sie stundenlang mit Produktvorführungen zum Kauf überteuerter Ware überzeugt werden sollen.

Prävention

- EC/Kreditkarte zuhause lassen
- Nur wenig Bargeld mitbringen
- Schwarze Liste im Vorfeld überprüfen https://www.vzhh.de/sites/default/files/medien/134/dokumente/Kaffeefahrten-Liste_19-09-13.pdf
- Nummernschild des PKW/Bus (Name des Busunternehmens) notieren
- Verkäufer*innen um Vorlage seines Personalausweises/seiner Visitenkarte bitten
- Handy mit sich führen, um im Notfall die Polizei zu verständigen

Was tun, wenn Sie Opfer geworden sind?

- Sollten Sie noch nicht bezahlt und nur eine schriftliche Bestellbestätigung erhalten haben, können Sie noch widerrufen.
- Kontaktieren Sie Ihren Anwalt. Versuchen Sie die Täuschung anzufechten sowie Nichtigkeit aufgrund von Wucher.

Kostenfallen

Kontaktaufnahme:
Briefkästen mit falschen Angeboten und personenbezogene Werbemails und Anrufe

Information

Hohe Kosten für ältere Kunden

Senioren*innen sind für manche Unternehmen lukrative Ziele. So werden etwa Unkenntnisse über die digitale Welt der Technik oder eine gutmütige Einstellung ausgenutzt, um Verträge abzuschließen.

Prävention

- Treffen Sie keine kurzschlüssigen Entscheidungen und fragen Sie nach Bedenkzeit.
- Suchen Sie sich Hilfe bei ihren Angehörigen/Nachbarn oder erkundigen Sie sich bei Ihrem Anwalt.
- Bleiben Sie stur und lassen Sie sich nicht „an der Haustür“ überreden.

Was tun, wenn Sie Opfer geworden sind?

- Kündigen Sie Ihren Vertrag zum nächstmöglichen Termin. Falls Sie dies nicht alleine können, bitten Sie Angehörige, Nachbarn um Hilfe. Folgende Informationen sollten enthalten sein: Vertragsnummer, Kündigung zum nächstmöglichen Zeitpunkt, Bitte um Bestätigung des Schreibens.
- Im Schlimmsten Fall: Kontaktieren Sie Ihre*n Anwalt*innen und versuchen Sie die Anfechtung wegen Täuschung, Zwangslage oder ein Mangel an Urteilsvermögen. Klagen Sie dann auf Nichtigkeit aufgrund von Sittenwidrigkeit. Dies gilt auch für überteuerte Käufe.

Enkeltrick

Kontaktaufnahme:

Meist über Telefon, seltener über Nachricht via SMS oder Messenger Diensten

Information

Es wird eine Krisensituation geschildert, die eine schnelle und vertrauensvolle Kommunikationsbasis schaffen sollen, z.B. in dieser Art:
"Ja hallo, ich bin es deine Enkelin. Ich hatte einen Unfall, ich bin verletzt, aber mir geht es gut. Da ich schuld war, brauche ich nun Geld. Der andere Mann muss operiert werden. Ich wollte kein großes Drama daraus machen."

Prävention

- Seinen sie immer skeptisch, wenn jemand Sie am Telefon um Geld bittet.
- Legen Sie einfach auf, wenn es Ihnen komisch vorkommt, etwas unlogisch oder nicht nachvollziehbar klingt und rufen Sie Ihren echten Enkel unter der von Ihnen eingespeicherten Nummer zurück.
- Übergeben Sie niemals Geld an eine Ihnen unbekannte Person.
- Prüfen Sie die Nachricht auf Satzbau- oder Grammatikfehler – es kann eine künstlich generierte Nachricht sein.

Was tun, wenn Sie Opfer geworden sind?

- Informieren Sie sofort die Polizei, wenn Sie Opfer geworden sind oder wenn Ihnen ein Anruf verdächtig vorkommt.
- Bei einer Nachricht: Melden Sie und markieren Sie diese als SPAM.

Gewinnspiel

Kontaktaufnahme:

Meist per Telefon, manchmal auch per E-Mail

Information

Plötzlich Millionär*in oder Zusatzrente?

Bei ihren Opfern behaupten Täter*innen, diese hätten eine große Summe, einen teuren PKW oder andere hochwertige Sachwerte gewonnen. Die Tücke: Die Überreichung kann nur gegen eine Bearbeitungsgebühr und durch die Angabe von personenbezogenen Daten ausgezahlt werden.

Prävention

- Sofern Sie nicht an einem Gewinnspiel teilgenommen haben sollten, können Sie auch nicht gewinnen.
- Zahlen Sie niemals Geld und geben Sie nie Ihre Bankdaten an, um einen Gewinn ausgezahlt zu bekommen.
- Geben Sie keine Details zu sich oder Familienmitgliedern preis.
- Fragen Sie die Anrufer*innen nach ihren Namen, der Firma, Adresse und Telefonnummer.
- Überprüfen Sie Ihre Kontoauszüge sowie Telefonrechnungen.
- Antworten Sie nicht auf Mails/SMS/WhatsApp, sondern melden Sie diese und verlegen Sie diese Nachrichten in Ihren „Spam“-Ordner.

Was tun, wenn Sie Opfer geworden sind?

- Rufen Sie die Polizei an, wenn Sie Opfer geworden sind und geben Sie eine Anzeige auf. Sammeln Sie dazu alle Beweise, z.B. ein Bild der Mail, sofern Sie die Nachricht via Mail/SMS/WhatsApp erhalten haben.
- Lassen Sie unberechtigte Abbuchungen von Ihrer Bank zurückeinfordern.

Internetbetrug

Kontaktaufnahme:

Anhänge in E-Mails. Unseriöse „fake“ Online-Shops. Unseriöse „fake“ Seiten; Imitation des Originals

Information

Betrug im Internet?

Im Internet kann man fast alles machen: Einkaufen gehen, Bankgeschäfte erledigen, aktuelle Nachrichten verfolgen u.v.m. Entscheiden Sie sich für die Nutzung von Internet, ist es umso wichtiger, sich gegen die möglichen Risiken vorzubereiten. Hier finden Sie ein paar Vorschläge, die Sie schützen.

Prävention

- Aktivieren Sie die sogenannte „Windows Firewall“ und führen Sie regelmäßig Virenscans durch.
- Halten Sie Ihre Softwares immer auf dem aktuellsten Stand.
- Erstellen Sie sichere Passwörter. Ein sicheres Passwort sollte mind. 8 Zeichen lang sein, Groß-, Kleinbuchstaben, Ziffern & Zeichen enthalten. Notieren Sie sich das Passwort, um es nicht zu vergessen.
- Bitte merken Sie: Keine Bankinstitute, Versicherungen oder Dienstleister verlangen von Ihnen wichtige persönliche, Bank- oder Login-Daten per Mail.
- Öffnen Sie keine Anhänge von unbekannten Email-Absendern.
- Nutzen Sie bei fremden PC/Laptops keine persönlichen Daten.
- Erhöhen Sie die Sicherheit Ihres Internet-Browsers.
- Vorsicht beim Download von Software aus dem Internet.
- Sichern Sie Ihre (drahtlose) WLAN-Verbindung (z.B. Ändern des Passwortes).
- Seien Sie mit der Angabe persönlicher Daten im Internet zurückhaltend.
- Schützen Sie Ihre Hardware gegen Diebstahl und unbefugten Zugriff.

Anlaufstellen

Melden sie sich bei der örtlichen Polizei! Informationen bekommen Sie unter 0800-274 1000 zwischen 8 und 18 Uhr.

Information

In eine Falle getappt?

Sie sind nicht alleine. Es gibt viele Anlaufstellen, über welche Sie Hilfe bekommen. Im Folgenden finden Sie die wichtigsten rund um digitale Betrugsmethoden.

Telefonisch

- Wenn Sie Opfer eines Verbrechens wurden, wenden Sie sich an die Polizei (110).
- Wenn Ihr Bankkonto gesperrt werden muss, hilft Ihnen neben Ihrer Bank auch der kostenlose Sperr-Notrufdienst weiter: 116 116.
- Kontakt für Kriminalitätsopfer: 069/252500
- Hilfetelefon für digitale Gewalt: 116 016 (für Frauen), 0800 123 99 00 (für Männer)
- Beratungsinformation der Darmstädter Hilfe: 06151/9714200

Weitere Hinweise:

- Existierendes Datenmaterial (E-Mails, Chat-Verläufe in Messenger-Diensten, digitale Fotos oder Videos u. v. m.) aufbewahren und unverändert lassen. Diese sind wichtige Beweismittel. Wenn möglich, abspeichern oder ausdrucken.
- Bei unbekannten Abbuchungen von Ihrem Konto treten Sie mit Ihrer Bank in Verbindung.
- In Ihrem Umkreis finden Sie weiterführende Informationen und Anlaufstellen auf: Hilfe-info.de.