Vortrag über Internet - Kriminalität

1. Erläuterung der bekanntesten Betrugsmaschen
2. Erkennen von Merkmalen des Betruges
3. Ziele des Täters und die Folgen eines Betruges
4. Umgang mit personenbezogenen Daten, Zugangsdaten und Kontaktdaten
5. Bezahldienste und Kontonummern
6. Fallbeispiele verschiedener Phänomenbereiche
7. Sichere Passwörter und E-Mail-Adressen
8. Persönlichkeitsrechte und Drohnen
9. Zusammenfassungen als Übersicht

Bezahldienst PayPal

Warenbetrug mittels Verkaufsportal www.kleinanzeigen.de

Täter bieten an, dass die Bezahlung per PayPal mit der Option „Freunde und Familie" erfolgt. In dem Fall entstehen zwar keine weiteren Kosten durch Gebühren, aber der „KÄUFERSCHUTZ" ist auch außer Kraft gesetzt. Betrüger bekommen quasi das Geld „geschenkt" und Sie erhalten keine Ware.

Täter benutzen natürlich keine Echtdaten von sich selbst. Sie erstellen entweder einen neuen Account bei www.kleinanzeigen.de mit erlangten Daten von geschädigten Personen aus anderen Straftaten oder sie haben einen Account von einem anderen Geschädigten „übernommen" (zuvor E-Mail „gehackt" und „Kennwort zurückgesetzt" oder den Server vom Betreiber direkt angegriffen oder Daten abgefangen).

Gastkonto - Betrugsmasche

Bei Online-Händlern wird die Bezahlmethode PAYPAL angeboten. Sie müssen nicht zwingend einen Account bei PAYPAL besitzen, sondern können bei den Händlern per GASTZUGANG über PayPal bezahlen. Für diese Option benötigen Sie lediglich die IBAN.

Täter erlangen ihre IBAN (Rechnung von der Firma, Kontoauszug der Bank, Überweisung bei Kauf, Datenleck bei Webseiten-Betreiber oder Firmen) und kaufen damit ein. Sie lassen sich die Ware an eine DHL Packstation senden (dort haben Sie Daten von gefälschten Ausweisen oder gestohlenen Ausweisen hinterlegt) oder direkt an eine Adresse (dort wird der Postbote angesprochen, dass man gerade erst hergezogen ist und am Postkasten wird ein falsches Namensschild der eigentlich leer stehenden Wohnung angebracht).

HINWEIS für Firmeninhaber und auch jeden Kontoinhaber

Besitzen Sie ein Bankkonto bei einer Bankgesellschaft und ihre IBAN ist nicht mit einem PAYPAL-Konto verknüpft, wird bei der Eingabe der IBAN als Gastkonto auch kein PASSWORT verlangt. Das bedeutet, jeder kann ihre IBAN für solche Zwecke missbrauchen.

Firmeninhaber versenden viele Rechnungen oder haben teilweise auf ihren Webseiten Kontodaten zur Bezahlung der Ware publiziert. Ist eine solche IBAN nicht mit einem PAYPAL-Konto verknüpft, laufen Sie Gefahr, dass diese missbräuchlich verwendet wird.

IBAN - EMPFÄNGER - ÜBERPRÜFUNG

Seit Oktober 2025 führen die Banken die IBAN - Empfänger - Überprüfung ein. Diese werden aber nur auf Überweisungen angewendet. Bei der Bezahlung mittels Gastkonto handelt es sich aber um eine Abbuchung im Lastschriftverkehr. Grundsätzlich hat man bei Abbuchungen 8 Wochen Widerspruchsfrist, aber bei „unberechtigten Abbuchungen" (Nachweis durch Erstattung Anzeige bei der Polizei verpflichtend) verlängert sich das Widerrufsrecht auf 13 Monate.

Eine Überweisung wird von einem selbst autorisiert durch Eingabe der Daten im Online-Banking oder Einwurf eines Überweisungsträgers bei der Bank. Beim Online-Banking findet inzwischen Sofort-Überweisung statt. Hier besteht kein Widerrufsrecht.

Unbekannte Nummer oder Nummer aus dem Ausland

VORSICHT !!! JA - SAGEN - METHODE

Anrufer fragt Sie ob sie bereits die neuesten Angebote zu Produkten wie Photovoltaikanlagen oder Lotto-Gewinnspielen kennen. Während des Gesprächs können Fragen kommen wie: „Verstehen Sie mich?". Dem Täter ist es wichtig, dass Sie „JA" sagen. Ihr Gespräch wird ohne ihre Erlaubnis und ihres Wissens aufgezeichnet und später verarbeitet.

Wenige Tage später erhalten Sie eine Rechnung über abgeschlossene Verträge, Abonnements oder Gewinnspielen. Mit dem falschen Telefonmitschnitt werden Sie zusätzlich konfrontiert und unter Druck gesetzt. Zudem erhalten Sie schreiben von Inkassobüros.

Die Aufgabe eines Inkassobüros ist es Mahnungen zu versenden, um die Forderungen des Gläubigers einzuholen. Oftmals werden Forderungen komplett an das Inkasso-Unternehmen abgetreten.

Es gibt jedoch auch Betrugsmaschen, bei denen solche Schreiben „Totalfälschungen" sind. Das Inkassobüro existiert gar nicht und durch Druck will man erreichen, dass Zahlungen auf das Konto des Täters eingehen.

Grundsätzlich gilt für jeden Bürger bei Verbraucherverträgen ein Widerrufsrecht gemäß § 355 BGB Die Widerspruchsfrist beträgt 14 Tage. Auch wenn Sie nicht sicher sind, ob das Schreiben „echt" ist, auf keinen Fall ignorieren. Immer einen Widerspruch versenden. Die rechtzeitige Absendung ist rechtswirksam

Sollten Sie einen Anruf von einer ausländischen Rufnummer erhalten, ist es sehr wahrscheinlich, dass die Täter von Ihnen Daten erlangen (angeblicher Mitarbeiter der Bank oder PayPal oder Microsoft - Mitarbeiter - VISHING) wollen oder es sich hierbei um einen

PING - Anruf handelt.

Bei einem PING - Anruf klingelt das Telefon nur kurz. Die Täter wollen erreichen, dass Sie zurückrufen. Sie werden automatisch an „kostenpflichtige teure Rufnummern" weitergeleitet. Die nächste Rechnung ihres Telefonanbieters wird höher als gewöhnlich sein.

Wie kann ich mich schützen?

1. Wenn Sie keinerlei Kontakte im Ausland pflegen, sperren Sie auf ihrem Smartphone oder in dem Router (z. B. FritzBox) eingehende Anrufe aus dem Ausland
2. Unbekannte Rufnummern nicht annehmen
3. Fragen immer mit Gegenfragen beantworten, aber niemals „JA" sagen.

Rechtslage:

Bei Dienstleistungsverträgen am Telefon (Verlängerung Mobilfunkvertrag) müssen Anbieter seit 01.Dezember 2021 eine Vertragszusammenfassung schriftlich nachreichen (auch E-Mail). Andere Verträge wie Warenverträge oder Abonnements Zeitschriften benötigen diese Zusammenfassung nicht. Gemäß § 125 BGB sind mündlich geschlossene Verträge rechtsgültig und bindend. Jedoch hat man immer noch das Widerrufsrecht innerhalb von 14 Tagen.

Das Mitschneiden des Telefongespräches ohne Zustimmung stellt grundsätzlich eine Straftat gemäß § 201 STGB (Vertraulichkeit des Wortes) dar, aber bei der Nachweisbarkeit ist schwierig, da die Zustimmung vor der Aufzeichnung erfolgt. Hier gilt auch bei Rechtsgrundsatz: „In dubio pro reo" also „im Zweifel für den Angeklagten".

Phänomenbereiche

Identitätsdiebstahl - Der Diebstahl ihrer Identität ist kein eigenständiges Delikt, aber die Erlangung bei Umgehung von Sicherheitsdiensten oder die missbräuchliche Verwendung erfüllen verschiedene Straftatbestände des Betruges (inkl. Computerbetrug) oder Fälschung beweiserheblicher Daten oder Datenveränderung (Passwort oder Umleitung E-Mails) oder Ausspähen von Daten.

Phishing - Betrüger senden gefälschte E-Mail von Banken, um Zugangsdaten zu erlangen (Druck wird aufgebaut -Kontosperrung angekündigt) oder gefälschte E-Mail von Postzusteller, um personenbezogene Daten und Bankdaten zu erlangen (Zeitdruck wird aufgebaut - sonst geht Ware zurück oder ansonsten werden Zollgebühren fällig)

Smishing - eine besondere Form von Phishing. Auch in dem Fall werden SMS oder WhatsApp genutzt, um an Daten zu gelangen. Falsche Nachrichten von Banken für Bestätigungen, Freischaltungen oder Aktualisierungen. Ziel ist die Erlangung der Zugangsdaten. Aber auch Nachrichten WhatsApp „Hallo MAMA...Neue Nummer" haben das Ziel Geld zu erlangen und zeitgleich die IBAN-Daten.

Quishing - die Form von Phishing arbeitet mit QR-Codes. Gefälschte Schreiben vom Amt im Briefkasten mit QR-Codes für Zahlungen. E-Mails von Banken mit QR-Codes. Aber auch außerhalb der digitalen Welt werden QR-Codes an Ladesäulen oder Parkgebühr-Automaten überklebt. Wenn solche QR-Codes gescannt werden, überweist man das Geld an das Konto der Täter und sie erlangen zeitgleich ihre Bankdaten. IBAN können missbräuchlich verwendet werden.

Vishing - Zusammensetzung aus Voice und Phishing. Betrüger kontaktieren den Geschädigten per Telefonanruf. Geschädigte werden kontaktiert und eine finanzielle Notlage eines Angehörigen wird vorgetäuscht, damit Geld bezahlt wird („Enkeltrick"). „Falscher Polizeibeamter" meldet sich und berichtet über Einbrüche in ihrer Umgebung. Zur Sicherheit wird „Bargeld" eingesammelt und bei der Polizei „verwahrt". Angeblicher Mitarbeiter von Microsoft hat Virus auf ihrem Computer festgestellt. Sie erhalten einen Code zur Eingabe und plötzlich öffnen sich unzählige Ereignisprotokolle. Es entsteht Panik und die Mitarbeiter bieten Ihnen zu helfen mittels Fernwartungssoftware. In dem Moment übernehmen Fremde ihren Computer oder ihr Smartphone (z. B. AnyDesk). Auch wenn sie ihre Passwörter im Browser wie Edge oder Firefox löschen, können bei direktem Zugriff immer alle Protokolle ausgelesen werden. Also auch alle Zugangsdaten ausgelesen werden.

Call-ID-Spoofing - Beim Vishing übermitteln die Täter selbstverständlich keine Echtdaten von sich. Vom Namen bis hin zur Rufnummer ist alles „falsch". Mittels Software werden andere Rufnummern „vorgetäuscht". Das könnte echte Rufnummern von Banken oder anderen Personen sein oder auch fiktive Daten.

IP-Spoofing - Die Software zur Manipulation von Rufnummern findet auch Anwendung bei IP-Adressen. Wenn das World Wide Web „betreten" wird, erhalten Sie von ihrem Provider eine freie dynamische IP-Adresse. Jeder Provider (Anbieter von Telefon- und Internetdiensten) hat nur ein begrenztes Kontingent an IP-Adressen. Deshalb rotieren diese und werden immer wieder neu zugewiesen. Aufgrund Flatrates ist es nicht mehr zu Abrechnungszwecken erforderlich diese IP-Protokolle zu speichern. Es findet somit keine Vorratsdatenspeicherung statt. Des Weiteren können Proxy-Server genutzt werden, um anonym im World Wide Web unterwegs zu sein.

VPN - Das Virtual Private Network ist kein Proxy Server zur Anonymisierung wie JAP, sondern dieser „Tunnel" verschlüsselt die Daten. Die verschlüsselten Daten gelangen somit sicher vom Sender zum Empfänger. Auch wenn diese Daten „abgefangen" werden, sind sie sicher. Ohne VPN, können Täter die gesendeten Daten (Zugangsdaten werden zur Bank gesendet) abgefangen werden. Besonders gefährlich, wenn sie öffentliche Netzwerke Hotel oder Bahnhof oder Flughafen nutzen.

Evil-Twin-Hotspots - Angreifer erstellen einen falschen Hotspots mit ähnlichem Namen z.B. anstatt „Telekom-ICE“ wird einer bereit gestellt mit „Telekom_-ICE“. Auch bei öffentlichen WLAN am Flughafen oder Hotels können Täter einfach ihre Daten mitlesen und abgreifen. Deshalb in solchen Netzwerken niemals persönliche Daten oder Zugangsdaten bei Banken oder Accounts verwenden.

Business E-Mail Compromise - Bei dieser Variante werden Rechnungen von E-Mails „abgefangen“ und „verändert“. Firma sendet Rechnung an Kunden. Kunde erhält kurz darauf eine weitere E-Mail mit der Bitte neue IBAN zu nutzen. Die Rechnung ist abermals als Anhang dabei. Lediglich die IBAN wurde ersetzt. Kunde zahlt nun an den Täter und nicht an die Firma. Das „Datenleck“ kann sowohl auf dem Netzwerk der Firma durch Schadsoftware stattgefunden haben, als auch auf dem Weg durch „abfangen“ (siehe VPN) oder die E-Mail des Empfänger und dessen „Server“ wurden bereits „gehackt“ und überwacht. Unbedingt alle E-Mails und HEADER sichern !!!

Love Scamming - Einsame Menschen lassen sich schnell zur Liebe verführen. Sie lernen im Internet einen Fremden kennen, der ihnen die Sterne ins Wohnzimmer bringt. Dieser wohlhabende Mensch mit einer wichtigen Funktion im Ausland (Arzt oder Manager) „gaukelt“ die große Liebe vor. Irgendwann hat die geliebte Person plötzlich finanzielle Schwierigkeiten, weil Konto gesperrt wurde oder Notfall in der Familie oder andere Gründe. Schwer verliebte Menschen überweisen viel Geld aus Liebe und Hilfsbereitschaft. Zudem wurde eine Rückzahlung versprochen mit einem dicken Bonus obendrauf.

Job Scamming - Täter bieten mit ihren Webseiten Jobs für zuhause an. Einfach und schnell Geld verdienen. Sie sollen Apps testen oder sogar Kreditangebote bei der Bank. Am Monatsende gibt es aber keinen Lohn, sondern die große Überraschung. Die Täter haben nicht nur ihre Daten erlangt (Arbeitsvertrag mit Kontodaten), sondern aufgenommene Test - Kredite müssen sie zurückzahlen und der Täter erhält das Geld. Mit den Kopien von ihrem Personalausweis werden weitere Straftaten begangen (Konto - Eröffnung und Geldwäsche). Sie werden bald zum Täter bei der Geldwäsche. NIEMALS Kopien oder Screenshots von AUSWEISEN weitergeben !!!

Warenagent - Auch in dem Fall erhalten Sie von den Tätern ein Job - Angebot. Aber dieses Mal arbeiten Sie tatsächlich. Sie arbeiten quasi als Subunternehmer für Betrüger. Ihnen werden Waren zugesendet. Sie sollen diese umverpacken und an eine andere Adresse (angebliche Tochterfirmen oder Endkunden). Dafür erhalten Sie einen Lohn. Täter betrügen über www.kleinanzeigen.de mit den erlangten Bankdaten, PayPal-Daten oder Ausweisdaten anderer Geschädigten weitere Menschen. Es werden immer mehr Daten erlangt. Mittels IBAN als Gastkonto PayPal bestellen Sie Waren und sie leiten diese weiter. Es werden Firmen und andere Leute betrogen und Sie werden zum Mittäter.

Finanzagent - Die gleiche Methode gibt es auch ohne Warensendungen. Sie nehmen einen Job als Finanzagent an. Ihnen wird Geld aus Betrugsmaschen zugesendet und sie haben die Aufgabe es an andere Täter zu verteilen. Sie werden quasi zum Buchhalter der Betrüger.

Gast-Account PayPal - Betrüger können mit ihren erlangten IBAN - Daten bei Firmen im Internet Waren bestellen. Wenn ihre IBAN nicht mit einem PAYPAL -Account verbunden ist, kann man als Gastkonto PayPal bestellen. Die Abbuchung erfolgt anschließend auf ihrem Konto. Ist ihr Konto verbunden, werden Sie bei Eingabe der IBAN automatisch gebeten, sich einzuloggen. Firmeninhaber haben oftmals Kontodaten auf Webseiten publiziert. Diese Konten sind nicht sicher, wenn sie keine Verbindung zu einem PayPal-Account haben.

Fake Shop - Eine Form des Warenbetruges. Sie kaufen über ein Verkaufsportal ebay oder kleinzeigen oder persönlich in einer Gruppe bei Facebook einen Artikel und erhalten diesen nicht. Das ist der klassische Warenbetrug. In dem Fall nutzen Täter eine eigene Webseite. Diese sieht täuschend echt aus. Sie finden diese Webseiten mittels Suchmaschinen oder wenn Sie auf Werbebanner klicken, werden Sie dorthin umgeleitet. Oftmals werden Webseiten von Firmen täuschend echt kopiert. Sie geben ihre personenbezogenen Daten, Kontaktdaten und Zahlungsdaten ein. Sie erhalten sogar E-Mails mit Rechnungen. Diese Webseiten sind im Internet bei Verbraucherzentralen oftmals bekannt und viele Warnmeldungen im Umlauf. Immer die DOMAIN exakt überprüfen.

Beispiel: www.vaude.com und Täter nutzt www.vaude-de.com

Fake Shops sind täuschend echt, aber oftmals sind diese telefonisch nicht erreichbar. Anrufbeantworter verweisen auf E-Mail-Kontakt. Bei Bezahlung per PayPal mit Käuferschutz unerwartet ohne Funktion und man wird um Sofortüberweisung gebeten.

Sexpressing - Täter versendet E-Mail mit der Aufforderung Geld zu bezahlen, da man angeblich pornografische Schriften angesehen und verbreitet hat. Die Schreiben sind angeblich von Überwachungsorganen, Behörden, Polizei oder Justiz. Es handelt sich hierbei um eine Erpressung. Auf keinen Fall bezahlen !!!

Sextortion - Bei der Variante von Erpressung, hat man tatsächlich mit einer anderen Person Kontakt aufgenommen. Über soziale Dienste und Messanger wie Facebook, Instagram und Whatsapp wird man von einer „scharfen" Lady oder dem „geilen" Typen angeschrieben. Die andere Person zeigt sich sehr verliebt und vor allem „offen" für alles. Man erhält anfangs Bilder und Videos von der interessanten Person und zwar ohne Bekleidung.

Ransomware - Computer wird durch BKA-Trojaner (angeblich durch BKA, BND, GSI, GVU, Bundespolizei, National Cybercrime,....) gesperrt. Entsperrung erfolgt nach Bezahlung von Geld in Höhe von 100 bis 250 Euro an Bezahldienst uCash und mittels PaySafeCards. Hierbei handelt es sich um eine Erpressung. Oftmals Vorgabe Zeitdruck bis Zahlung erfolgen muss. Bei einer Attacke mit Javascript, ist meistens nur ein Neustart des Computers erforderlich. Sollte aber eine SCAREWARE (=Schadsoftware) Infektion vorliegen, sollte eine Systemwiederherstellung durchgeführt werden.

Öffentliches WLAN - Frei zugängliche WLAN - Netzwerke am Bahnhof, im Hotel oder am Flughafen oder auch bei Fast-Food-Ketten sollten niemals für Anfragen bei Banken genutzt werden oder auch zum Abruf von E-Mails. Jeder in dem WLAN -Netzwerk kann mittels Software die Daten „abfangen". Vor allem, wenn keine VPN - Verschlüsselung verwendet wird, sind die Daten frei verfügbar.

Evil-Twin-Hotspot - Ein Hotspot der Telekom wird angeboten und der Täter erstellt ebenfalls einen Hotspot mit ähnlicher Bezeichnung z. B. TelekomICE und Telekom_ICE. Der Geschädigte loggt sich ins Netzwerk der Täter ein und alle Daten werden erlangt. Es können sogar aktive Angriffe mit Schadsoftware auf technische Geräte durchgeführt werden, ohne es mitzubekommen.

Social Engineering - Der Mensch wird überzeugt Daten weiterzugeben. Beim Computerbetrug hingegen wird das Gerät selbst überlistet. Alle Formen von Phishing an denen Menschen beteiligt sind, sowie auch bei Erpressungen wie Scareware und Sextortion, aber auch Baiting (USB-Stick mit Schadsoftware wird an PC angeschlossen) und Waterholing (oft besuchte Seiten werden mit Malware infiziert - Werbebanner mit Link zur Webseite des Täters) gehören zu dem Oberbegriff.

Transportkostentrick - Betrüger zeigt Interesse einen angebotenen sperrigen Gegenstand zu kaufen. Er will die Ware auch abholen. Plötzlich ist der Käufer verhindert und bietet an, dass der Gegenstand von einer Spedition abgeholt wird. Anschließend erhält der Käufer eine E-Mail mit einem gefälschten Überweisungsbeleg oder eine E-Mail von einer Bank als Bestätigung der Zahlung. Laut Beleg hat der Käufer (Betrüger) den Kaufbetrag inklusive Transportkosten an den Verkäufer (Geschädigten) überwiesen. Nun überweist der Geschädigte den Betrag für die Transportkosten an den Spediteur (meist mit Sitz im Ausland). Jedoch ist der Spediteur zeitgleich der Betrüger. Kurz darauf erkennt der Verkäufer, dass er die Transportkosten bezahlt hat, aber der Überweisungsbeleg gefälscht war und gar keine Zahlung auf sein Konto eingegangen ist.

Kreditkartenproblem - Käufer bei www.kleinanzeigen.de erklärt, dass die Bezahlung per Kreditkarte fehlgeschlagen ist. Verkäufer erhält Link von www.kleinanzeigen.de (täuschend echt, aber vom Betrüger) für die Eingabe seiner Kreditkarten samt Prüfziffer, damit Zahlung erfolgen kann. In dem Moment erhalten Betrüger ihre Daten und können damit einkaufen gehen.

Betrug mit dem Scheck - Betrüger meldet sich aufgrund einer Verkaufsanzeige. Anschließend sendet er einen Scheck mit dem Kaufbetrag plus mehrere hundert Euro darüber. Angeblich wurde versehentlich falscher Betrag eingetragen und dadurch entsteht eine finanzielle Notlage. Verkäufer wird aufgefordert den zu viel bezahlten Betrag zurück zu zahlen. Der Scheck platzt erst Wochen danach und am Ende hat der Verkäufer seine Ware noch, aber die Differenz (versehentliche Überbezahlung) wurde an den Betrüger geschenkt.

Dreiecksbetrug

Fall 1: Sie bestellen über soziale Medien (Chatrooms und Gruppen) oder einer Webseite (Fake Shops) eine Ware. Zwecks Erhalt der Waren geben Sie ihre personenbezogenen Daten (Lieferanschrift) an. Der Täter benutzt ihre Daten und bestellt damit bei einer Firma ihre geforderte Ware und lässt sie an ihre Adresse ausliefern. Sie bezahlen die Ware, indem Sie das Geld an den Täter überweisen. Bis dahin war Ihnen nicht bekannt, dass nicht der Täter, sondern eine andere Firma die Ware geliefert hat. Anschließend erhalten Sie eine Zahlungsaufforderung, Mahnung oder Schreiben vom Inkasso-Büro, da Sie ihre Ware bei der Firma nicht bezahlt haben. In dem Moment fällt der Betrug erst auf.

Fall 2: Sie bieten über www.kleinanzeigen.de einen Gegenstand zum Verkauf an. Der Betrüger heuchelt Interesse daran und sie werden sich handelseinig. Zeitgleich bietet der Betrüger ihren Gegenstand über eine andere oder gleiche Plattform zum Verkauf an. Ein Interessent meldet sich beim Betrüger. Auch diese werden sich handelseinig. Der Betrüger teilt dem Interessenten mit, dass Geld per PayPal an Sie zu überweisen. Nachdem Sie das Geld erhalten haben, versenden Sie die Ware an den Betrüger, aber bezahlt hat nicht er, sondern der Interessent. Anhand ihrer Daten bei PayPal wurden Sie als Betrüger in Sachen Warenbetrug ermittelt. Dabei haben Sie nichts von der dritten Person gewusst und dachten, dass Geld kommt vom Betrüger. Dieser hat nun die Ware von Ihnen erhalten und Sie müssen das Geld an den Interessenten zurückzahlen.

WhatsApp

Fall 1: „HALLO MAMA“ - Nachricht. Betrüger geben sich als ihr Kind aus und erklären, dass sie eine neue Rufnummer haben. Der Betrüger gibt an, dass sein Smartphone verloren ging und deshalb sein Bankkonto gesperrt wurde. Jedoch hat er dringend ein neues Smartphone benötigt. Seine MAMA wird nun gebeten, das neue Smartphone zu bezahlen. Das Geld wird angeblich später zurückgezahlt. Der Betrüger ist natürlich kein naher Verwandter von Ihnen und will lediglich das Geld erhalten und auch ihre IBAN für mögliche Einkäufe via Gast-Account PayPal.

Fall 2: Sie erhalten eine Bestätigungs-SMS angeblich vom WhatsApp Service Dienst. Die Identität ist jedoch vorgetäuscht (SpoofID), auch wenn WhatsApp als Absender angezeigt wird. Insbesondere kommen auch „Chatbots“ zum Einsatz. Mittels KI wird Ihnen vorgegaukelt, dass Sie einen Online-Kundenservice nutzen. Diese Bots geben vor, dass eine Sicherheitsprüfung oder Updates erforderlich sind. Der Bot führt mit Ihnen Gespräche in Echtzeit und das einzige Ziel des Bots sind die Erlangung ihrer sensiblen Daten. Niemals Zugangsdaten oder personenbezogene Daten oder Kontaktdaten eingeben !!!

Skimming - Bei Geldautomaten im Ausland ist besondere Vorsicht geboten. In Deutschland wurden beinahe alle Geldautomaten (außer in Berlin) betrugssicher gemacht. Das Auflegen einer falschen Tastatur oder das Anbringen eines Lesegerätes am Automaten ist durch den Betrüger in Deutschland eigentlich nicht mehr möglich. Jedoch im Ausland sind keine besonderen Sicherheiten (grüne Abdeckung Kartenlesegerät am Automaten) vorhanden. Die Betrüger können durch oben genannte Gegenstände spielend einfach die Daten ihre Bankkarten auslesen. Die Daten können online verwendet werden oder es können sogar neue Bankkarten mit den Daten erstellt werden. Auch bei manipulierten POS - Terminals (Zahlungsgeräte bei Verbrauchermärkten) können diese Daten erlangt werden. Solch manipulierte Geräte werden unbemerkt gegen das Echte vor Ort ausgetauscht. Oftmals im Ausland.

E-Mail - Passwörter und Hashes - Erlangung von Daten

Empfehlung: mindestens drei E-Mail-Adressen bei drei verschiedenen Providern (T-Online, GMX, Web, Protonmail, AOL, freenet, usw.)

1. E-Mail-Adresse für Kommunikation mit unbekannten Anbietern und Gesellschaften
2. E-Mail-Adresse für die Registrierung bei vertrauenswürdigen Webseiten
3. E-Mail-Adresse ausschließlich für die Nutzung von Bezahldiensten (z. B. PayPal)
4. E-Mail-Adresse (für Smartphone-Nutzer)

Gelangt der Täter in irgendeiner Form an ihre E-Mail-Adresse (z. B. Kontaktaufnahme bei Fakeshops, Chat bezüglich Angebote bei www.kleinanzeigen.de, etc), kann der Täter bei Verkaufsplattformen wie Amazon, ebay, Kleinanzeigen, usw. diese E-Mail-Adresse mit einem „falschen" Passwort eingeben. Täter erhält Mitteilung, dass „Passwort falsch ist", also ist bekannt, dass ein Account existiert. Nun braucht er nur noch die E-Mail „hacken" oder das Passwort abfangen oder den Server des Provider angreifen.

Sobald er die E-Mail „gehackt" hat, aktiviert er dort eine Umleitung auf eine andere E-Mail-Adresse (Datenveränderung). Nun muss der Täter nur noch „Kennwort vergessen - zurücksetzen" nutzen und schon hat er alle Zugänge zu Ihren Verkaufsportalen. Deshalb benötigen Sie mehrere E-Mail-Adressen. Nutzen Sie nur eine einzige E-Mail-Adresse, ist die Gefahr „Opfer von Cybercrime" zu werden wesentlich erhöht.

Kennwörter und Sicherheit:

Jedes Kennwort wird mittels eines Algorithmus (verschiedene mathematische Formeln) in einen sogenannten HASH umgewandelt. Dieser Hash sieht wie folgt aus:

„7c6a180b36896a0a8c02787eeafb0e4c" entspricht dem Passwort „password1"

1. Wörter aus einem Wörterbuch in jeder Sprache der Welt werden in 15 Sekunden problemlos erkannt
2. Wörter aus einem Wörterbuch ergänzt mit Zahlen werden unter 5 Minuten „geknackt"

Wie erlangt der Täter mein Passwort:

1. Eine Software testet alle Kombinationen von Wörtern in allen Sprachen der Welt und gleicht den erstellten HASH mit dem HASH-Wert ihrem Passwort ab. Sobald diese übereinstimmen, ist das Passwort erlangt.
2. Phishing - per E-Mail oder SMS, Chat oder Webseiten werden Daten angefragt und von Ihnen übermittelt
3. Spezielle Software (Spyware, Client, Viren, Trojaner, Würmer, App wie AirDroid, TeamViewer oder AnyDesk, Splashtop) erlauben Zugriff auf ihren PC, Laptop oder auf das Smartphone. Passwörter werden bei der Eingabe mitgelesen und an den Täter versandt

Sichere Passwörter und unendlich viele Passwörter für unzählige Webseiten:

1. Benutzen Sie keine Wörter vom Wörterbuch. Schreiben Sie diese absichtlich falsch. Anstatt „KATZE" schreiben Sie einfach „Chaättze"
2. Nutzen Sie immer ein bis mehrere Sonderzeichen, sowie mindestens drei Zahlen
3. Das Passwort darf nicht weniger als 8 Zeichen haben

Beispiel Kennwörter für Webseiten Amazon, ebay, Kleinanzeigen

ChaättzeAMAZ*123Hüummdd, ChaättzeEBAY*123Hüummdd, ChaättzeKLEI*123Hüummdd

Mit diesem System können Sie sich unendlich viele Passwörter merken !!!

Personenbezogene Daten

allgemeine Personendaten
(Name, Geburtsdatum und Alter, Geburtsort, Anschrift, E-Mail-Adresse, Telefonnummer, Foto, Ausbildung, Beruf, Familienstand, Staatsangehörigkeit, religiöse oder politische Einstellungen, Sexualität, Gesundheitsdaten, Urlaubsplanung, Vorstrafen)

Kennnummern
(Sozialversicherungsnummer, Steueridentifikationsnummer, Krankenversicherungsnummer, Personalausweisnummer, Matrikelnummer usf.)

Bankdaten
(Kontonummer, Kreditinformationen, Kontostände usf.)

Onlinedaten
(IP-Adresse, Standortdaten usf.)

physische Merkmale
(Geschlecht, Haut-, Haar- und Augenfarbe, Statur, Kleidergröße usf.)

Besitzmerkmale
(Fahrzeug- und Immobilieneigentum, Grundbucheintragung, Kfz-Kennzeichen, Zulassungsdaten usf.)

Kundendaten
(Bestellungen, Adressdaten, Kontodaten, usf.)

Werturteile
(Schul- und Arbeitszeugnisse usf.)

sachliche Verhältnisse
(Einkommen, Kapitalvermögen, Schulden, Eigentum (Haus, Wohung, Auto etc.)

bestimmbare Daten, d.h. erst mit weiteren Informationen kann man auf eine Person rückschließen (Personalnummer, IP-Adresse, Kfz-Nummer usf.)

Drohnen im Wohngebiet

1. Wer darf eine Drohne fliegen lassen?

Eine Drohne ist ein unbemanntes Flugobjekt. Seit 01.01.2024 sind Drohnen in Klassen eingeteilt. Ältere Drohnen nennt man Bestandsdrohnen. Zum Fliegen bzw. Steuern muss man das Mindestalter von 16 Jahren haben. Gegenstände dürfen nicht transportiert werden.

Jede Drohne benötigt eine Haftpflichtversicherung. Eine Drohne mit einer Kamera (unabhängig vom Gewicht) muss beim Luftfahrtbundesamt registriert werden. Dem Nutzer wird eine Piloten-ID zugewiesen, welche auf all seinen Fluggeräten sichtbar angebracht werden muss.

2. Wo darf die Drohne eingesetzt werden bzw. fliegen?

Hierfür wurden die sogenannten Manöver – Kategorien eingeführt. Flughöhe und Flugabstand werden hier definiert, jedoch müssen weiterhin Datenschutz und Persönlichkeitsreichte beachtet werden. Für den Privaten Nutzer sind folgende MANÖVER Kategorien OPEN A1 bis A3 entscheidend.

A1: Höchstzulässige Startmasse unter 900 Gramm
Die Drohne darf an unbeteiligte Personen heranfliegen, diese jedoch nicht überfliegen.

- **Bestandsdrohnen (vor 01.01.2024 mit einem Gewicht unter 250 Gramm)**
- **Drohne Klasse C0 (bis 250 Gramm)**
- **Drohne Klasse C1 (bis 900 Gramm)**

A2: Höchstzulässige Startmasse bis vier Kilogramm
Die Drohne darf bis zu 30 Meter an unbeteiligte Personen heranfliegen. Im „Langsamflugmodus" muss der Abstand mindestens fünf Meter betragen.

- **Drohne C2 (bis 4000 Gramm mit Pilotenzeugnis A2)**

A3: Höchstzulässige Startmasse unter 25 Kilogramm
Die Drohne muss einen Mindestabstand von 150 Metern zu Wohn-, Gewerbe-, Industrie- oder Erholungsgebieten einhalten.

- **Bestandsdrohnen (vor 01.01.2024 mit einem Gewicht ab 250 Gramm)**
- **Drohne C2**
- **Drohnen C3 bis C6**

3. Drohnen – Führerschein

Ein Drohnenführerschein A1/A3 kann online gegen Gebühr erworben werden. Drohnen über 250 Gramm Gewicht (Drohnenklasse C1 oder höher, sowie Bestandsdrohnen über 250 Gramm) dürfen nur mit einem Drohnenführerschein sowohl privat als auch gewerblich eingesetzt werden.

Ein Pilotenzeugnis A2 ist für alle Drohnen über 4000 Gramm erforderlich. Dies betrifft Drohnenklassen C3 bis C6, welche im privaten Bereich üblicherweise nicht zum Einsatz kommen.

4. Verbotszonen

- Gemäß § 21h Luftverordnung:

  Flughäfen 1 KM Abstand und zur Landebahn 5 KM auf 2 KM Breite
  Flugplätze 1,5 KM Abstand

- Drohnen dürfen nicht über 120 Meter Höhe geflogen werden. Verstöße werden mit Geldbußen geahndet. Flugdaten des registrierten Piloten werden gespeichert.

- Für Autobahnen und Schienenverkehr gelten die Regelungen nach EASA Guidelines. Des Weiteren kann man über verschiedene Apps wie „Droniq" Verbotszonen anzeigen lassen. Der Überflug von Straßen sollte grundsätzlich vermieden werden.

5. Persönlichkeitsrechte (Recht am eigenen Bild)

Auch wenn die Manöver – Kategorie OPEN A1 das Fliegen der Drohne nah am Menschen erlaubt, ist die Aufnahme von Fotos und Videos ohne deren Zustimmung grundsätzlich verboten. Die EU-Drohnenverordnung und die Flug-Verordnung regeln nicht den Datenschutz.

Wer Aufnahmen (Bilder oder Videos) von Personen ohne deren Zustimmung anfertigt, kann zivilrechtlich von den Betroffenen auf hohe Entschädigungszahlungen verklagt werden.

Werden solche Aufnahmen über soziale Medien (z.B. Facebook, Instagram, Tik Tok) oder Messanger – Dienste (Whatsapp etc) verbreitet (einmaliges Verschicken ausreichend), kann eine Anzeige wegen der Ordnungswidrigkeit gemäß §§ 22, 23, 33 Kunsturheberrechtsgesetz erstattet werden. Geldbußen bis 50.000 Euro möglich.

Wer Aufnahmen von Personen bei einem Unfallereignis, einer Notlage oder im höchstpersönlichen Lebensbereich (z. B. Aufnahme durch das Fenster im Badezimmer) anfertigt (verbreiten nicht erforderlich) begeht eine Straftat gemäß § 201a Strafgesetzbuch. Geldstrafe und Freiheitsstrafe bis 2 Jahre möglich.

JEDE DROHNE DARF NUR IN SICHTWEITE DES NUTZERS GEFLOGEN WERDEN !!!

Dienststelle
Polizeiinspektion **Neustadt an der Aisch** **Bahnhofstraße 43** **91413 Neustadt a.d.Aisch**

Aktenzeichen		
Sammelaktenzeichen		Fallnummer
Sachbearbeitung durch (Name, Amtsbezeichnung)		
Sachbearbeitung Telefon **09161/8853-0**	Nebenstelle **0**	Fax **20**

„KUNO"-Merkblatt zur Aushändigung an den/die Anzeigenerstatter(in)

Belehrung

Sie wurden informiert, dass die u. g. Karten-/Kontodaten, aber keine weiteren Daten zu Ihrer Person, durch die Polizei an die **EHI Retail Institute GmbH - Zentraler KUNO-Sperrdienst für Debitkarten** und von dort an die Kassensysteme des Einzelhandels weitergeleitet werden.

Durch Ihre Anzeige wird Ihre Karte bzw. werden Ihre Karten zunächst für 10 Tage befristet gesperrt. Um die entwendeten bzw. abhanden gekommenen Debitkarten über diesen Zeitraum hinaus dauerhaft sperren zu können, werden Sie um Mitteilung der **Kartenfolgenummer** gebeten. Hierbei wird Ihre entwendete/verlorene Karte bis zum Ablauf ihrer Gültigkeit im elektronischen Lastschriftverfahren gesperrt.

Ihnen bleiben dadurch zeitaufwändige Erklärungen gegenüber Ihrer Bank und ggf. zu veranlassende Rückbuchungen erspart. Ohne die dauerhafte Sperrung der Karte ist ihre Verwendung im Lastschriftverfahren (Bezahlung mit Unterschrift ohne Eingabe einer PIN-Nummer) bis zum Ablauf der Kartengültigkeit (i. d. R. mehrere Jahre nach Ausstellung der Karte) zu Lasten Ihres Kontos möglich.

Die verschiedenen Debitkarten zu einem Konto werden durch die Kartenfolgenummer unterschieden. Diese ist **einstellig** und nur auf dem Magnetstreifen hinterlegt. Auf manchen Kaufbelegen wird sie als Kartenfolgenummer mit aufgedruckt. Auch bei Geldautomatenabhebungen ist sie als einzeln stehende Ziffer nach der Bankleitzahl auf dem Kontoauszug angeführt.

Beispiele, wo sich die Kartenfolgenummer befinden kann, finden Sie unten auf diesem Merkblatt.

Selbstverständlich können Sie die Kartenfolgenummer auch bei Ihrer Bank erfragen.

Zur Nachmeldung der Kartenfolgenummer sowie zur Aufhebung der Sperre gibt es folgende Möglichkeiten:

- beim Zentralen KUNO-Sperrdienst der EHI Retail Institute GmbH
  Internet: **https://www.kuno-sperrdienst.de** (kostenlos) **oder**
  Telefon: **0800 - 1044403** (kostenlos aus dem deutschen Fest- und Mobilfunknetz)
  Montag bis Freitag von 08:00 Uhr bis 20:00 Uhr und Samstag von 08:00 Uhr bis 16:00 Uhr
- bei Ihrer aufnehmenden/nächsten bayerischen Polizeidienststelle (persönliches Erscheinen erforderlich)*

In allen Fällen ist die Angabe der **Sperrbestätigungsnummer** notwendig (siehe rechte Spalte der Tabelle)!

Entwendete/verlorene Debitkarten (früher ec-Karten)

Bankleitzahl (8-stellig)	Kontonummer (max. 10-stellig)	Folge-Nr. (1-stellig)	Name und Sitz der Bank	**Sperrbestätigungsnr.** (5-stellig)

Die KUNO-Sperrung durch die Polizei befreit den/die rechtmäßige(n) Karteninhaber(in) nicht von seiner/ihrer Verpflichtung gegenüber seiner/ihrer kontoführenden Bank bzw. Sparkasse, unverzüglich die Sperrung der verlorenen/gestohlenen Zahlungskarten bei dieser oder den zentralen Sperrannahmen (für Debitkarten siehe unten) auch für das PIN-Verfahren (electronic cash) vorzunehmen.

Beispiele, wo Sie Ihre Kartenfolgenummer finden können

GA NR00000012 BLZ70112345 **9**
13.09/07.54UHR MUSTERSTADT
EUR 200,00 GEB.EUR 2,05

MUSTERFIRMA AG
ELV90584532 15.09 09.47 ME**9**

Musterfirma GmbH
HAUPTSTR. 1
12345 Musterstadt
012/12345-0

Kto.12345678/0012345678

Karte **9** gültig bis 12/04
AID-Parameter 00951032A
AID 0074FAA

Sperrnummern: (Alle Angaben ohne Gewähr)

Sperr-Notruf 116 116 (gebührenfrei aus dem dt. Festnetz oder über Mobilfunk innerhalb Deutschlands)

Sofern sich Ihr Kartenherausgeber nicht dem **Sperr-Notruf 116 116** angeschlossen hat, verwenden Sie zur Sperrung der **Debitkarte** (früher ec-Karte) bitte folgende Rufnummer: **+ 49 - 1805 - 021 021** (gebührenpflichtig)

Weitere Informationen zur Kartensperre finden Sie auch unter: www.polizei-beratung.de

rrsrsrsssrrsssrsssrsrs-

* Bei Minderjährigen und betreuten Personen wird um Begleitung eines unterschriftberechtigten gesetzlichen Vertreters (Eltern, Betreuer, o. ä.) gebeten.

Interessante YouTube Videos

Paypal-Betrug: Wie Kriminelle mit dieser Masche abkassieren	Stern TV
Betrug und Geldwäsche: Abzocke bei der Arbeitssuche	Die Spur
Wie man Passwörter knackt (und wie du es verhinderst) - IT Security	Programmieren lernen
Erkenne Fake-Shops im Internet	m3
Lastschrift-Betrug: Wenn unbemerkt Geld vom Konto abfließt	ARD Marktcheck
Phishing: 45000 Euro geklaut trotz Konto-Sperrung	ARD Marktcheck
Betrug mit QR-Codes: Achtung , Phishing!	ARD Marktcheck
Die Deals von PayPal, Klarna und Co. - Wer macht das Geschäft	ZDF heute Nachrichten
Bezahlen mit dem Handy: Wie sicher sind Apple Pay und Google Pay	Turn On
SIM Swapping: Wenn Betrüger das Handy übernehmen	ARD Marktcheck
Anruf von angeblichen Bankmitarbeiter: Perfide neue Betrugsmasche	ARD Marktcheck
Handy-Betrug: Wenn der Angerufene zahlen muss (PING Anrufe)	ARD Marktcheck
Vorsicht Betrug, falsche Inkassofoderungen entlarvt! Schütze dich jetzt	Callcenter Abzocke
Jura Basics: Was dürfen Inkassobüros und was nicht?	WBS Legal
So gehen Betrüger bei ebay-kleinanzeigen vor	ARD Marktcheck