DU HAST NOCH FRAGEN?
MELDE DICH GERNE BEI UNS!

MAIL: LINDEMANN@M2C-BREMEN.DE
TEL: +49 176 57880024
WEB: IMPACT-LAB.EU/SPI

digital impact lab

RATGEBER: BETRUG

Unsere Unterstützer:

HAPNET

Freie Hansestadt Bremen

Co-funded by the European Union

M 2 C

INHALT

1. WAS DICH ERWARTET

Mit diesem Heft wollen wir dir gängige Betrugsmaschen erklären und dir zeigen, wie du dich dagegen schützen kannst.
Dabei werden wir dir alles so einfach wie möglich erklären, und dir bestmöglich helfen, dich gegen Betrug zu schützen.
Dabei ist unsere beste Chance, dir alle gängigen Betrugsarten zu zeigen und wie du dich gegen diese schützen kannst.
So kannst auch du anderen helfen besser geschützt sein, besonders in Zeiten des Internets ist das wichtig.

2. WAS IST EIGENTLICH BETRUG?

Sinngemäß ist laut dem Strafgesetzbuch Betrug, wenn jemand durch Lügen, das Verändern von wichtigen Informationen oder das Verheimlichen von wahren Tatsachen versucht, sich selbst oder jemand anderen Geld oder Besitz zu verschaffen.
Da sich Betrug und die Art wie Betrüger vorgehen ständig ändert, ist es wichtig immer wachsam zu sein und sich zu informieren.
In Zeiten des Internets wird auch das Synonym „Scam" für Betrug immer präsenter.
Heutzutage findet Betrug viel über elektronische Geräte und über das Internet statt, das bringt ganz neue Gefahren mit sich, da oft Daten und große Summen Geld auf dem Spiel stehen.

digital impact lab

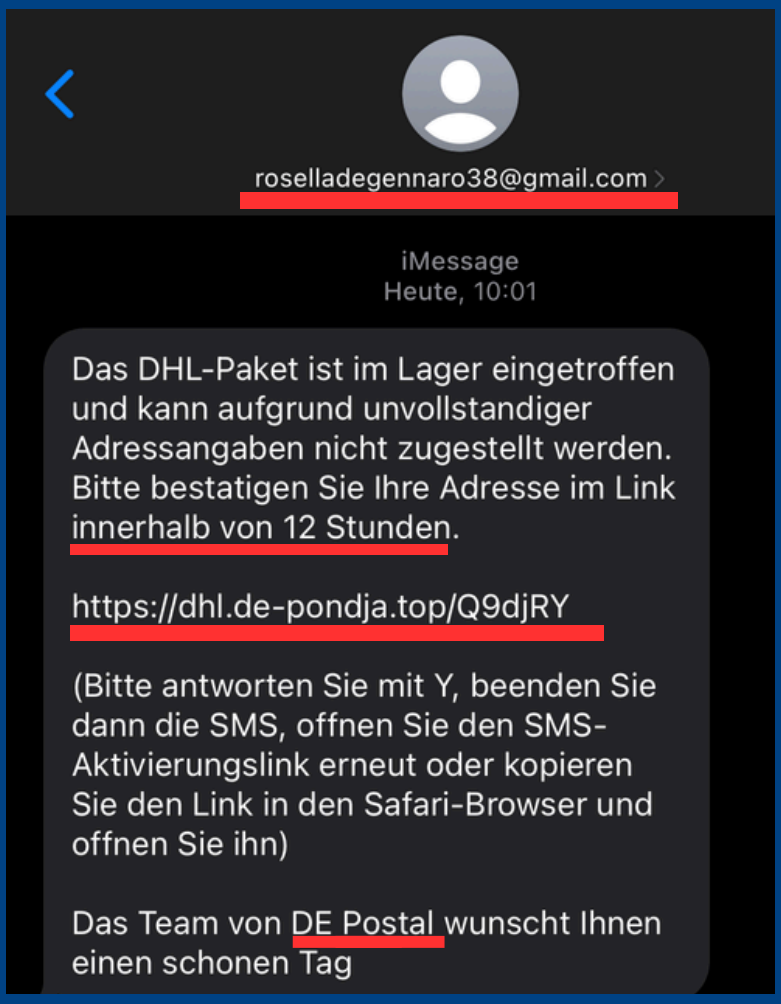
3. AKTUELLE BETRUGSARTEN

3. PHISHING: DEFINITION

Phishing, abgeleitet von „fishing“ (engl. Angeln), ist der Versuch, dich über gefälschte Webseiten, E-Mails oder Kurznachrichten zu täuschen.
Der Betrüger gibt sich als vertrauenswürdige Person aus, um an deine persönlichen Daten zu gelangen. Typischerweise sollst du dich auf einer nachgebauten Fake-Webseite einloggen, wodurch der Betrüger an deine Zugangsdaten kommt. Diese nutzt er dann, um dein Konto zu plündern oder andere betrügerische Aktivitäten, wie dem Verkauf der Daten, durchzuführen.
Phishing ist eine Form des Social Engineering, bei der deine Gutgläubigkeit ausgenutzt wird.

3. PHISHING: BEISPIEL

1. Beispiel:



Eine SMS von angeblich DHL, welche darauf hinweist, dass ein Paket zur Abholung bereitliegt, Zoll bezahlt werden muss oder sonstige Probleme auftreten und man deshalb auf einen Link klicken sollte. Weder DHL noch die Deutsche Post haben etwas damit zu tun.

3. PHISHING: BEISPIEL

2. Beispiel:

In dieser Nachricht wird dem Betroffenen vermittelt, dass dieser sich beeilen muss und sonst der Bankzugang gesperrt wird. Es ist keine andere Möglichkeit angegeben, zum Beispiel die App oder die Website selbst aufzusuchen, ohne Link. Deshalb handelt es sich um eine falsche Sparkassenmail.

3. PHISHING: ERKENNEN

Die Betrüger drängen oft zu einem schnellen Handeln unter anderem mit Drohungen.
Ein Beispiel wäre: „Gebe deine Daten an oder dein Konto ist morgen gesperrt."
Außerdem werden vertrauliche Daten und Informationen verlangt, dabei muss man besonders aufpassen, da das das Ziel der Betrüger ist. Die Daten werden in der Regel nicht über Mail abgefragt. Stattdessen muss die Identität zuvor bestätigt werden und meist kommen wiederholt Mails mit Aufforderungen und nicht mit Drohungen.
Beim Bestätigen der Identität durch eine Form des Einloggens wird man in den Mails größtenteils über Links auf falsche Websites geleitet. ...

3. PHISHING: ERKENNEN

Diese heißen ähnlich wie die echten Websites, sind jedoch nur dazu da, um die Einlogdaten des Opfers zu bekommen.
Hier muss man besonders darauf achten, dass die Website korrekt ist, am besten geht man jedoch nicht einmal auf den Link, denn dieser kann auch das elektronische Gerät mit Viren befallen. Wir empfehlen, dass die echte Website von dir aufgerufen wird und du dich dort einloggst und nach dem in der Nachricht betitelten Problem guckst.
Die Mailadressen können falsch sein, wenn du auf den Absender klickst und die dortige Mailadresse mit der vorher angezeigten vergleichst, können Unterschiede auftreten und es handelt sich in dem Fall um einen Betrüger. ...

3. PHISHING: ERKENNEN

Auch wenn es sich um vermeintliche Berühmtheiten oder große Organisationen handelt, sollte man vorsichtig sein. Ist das Anliegen des Senders ungewöhnlich oder unerwartet, wie ein vermeintliches Paket im Zoll, obwohl du kein Paket bestellt hast? Dann handelt es sich vermutlich auch um einen Betrüger. Des Weiteren kann man auch auf die Rechtschreibung und Grammatik achten, oft sind die Nachrichten aus dem Ausland oder schnell geschrieben, wodurch es zu einfach Fehlern kommt kann.

3. ONLINE BETRUG: DEFINITION

Online Betrug findet, wie der Name schon sagt, online statt. Speziell ist Online Betrug als Betrug über das Internet und mithilfe von falschen Inhalten definiert.
Die Betrüger melden sich oft über Nachrichten oder Mail als Werbung und leiten dich danach auf eine Website weiter oder du findest die Website bzw. Anzeige zufällig bei deiner Suche nach bestimmten Produkten oder Rabatten.

Die Websites oder Anzeigen verkaufen Produkte oder Dienste, diese existieren nicht, wenn nun dort gekauft wird, profitieren die Betrüger und du erhältst keine Gegenleistung. Dabei arbeiten die Betrüger zum Teil auch auf großen Online-Plattformen, mit falschen Angaben. Dort versuchen sie meist, auf andere Dienste und Zahlungsmethoden umzusteigen, damit sie schwerer zu verfolgen sind.

3. ONLINE BETRUG: BEISPIEL

1. Beispiel:

Stell dir vor, du willst dir einen neuen Laptop kaufen. Das Modell, das du haben möchtest, gibt es nicht mehr im Laden oder bei den bekannten online Händlern. Du findest den Laptop zu einem guten Preis bei einem kleinen online Handel. Du kaust schnell den Laptop, bevor er weg ist. Dein Laptop kommt nicht an und dein Geld ist weg.

2. Beispiel:

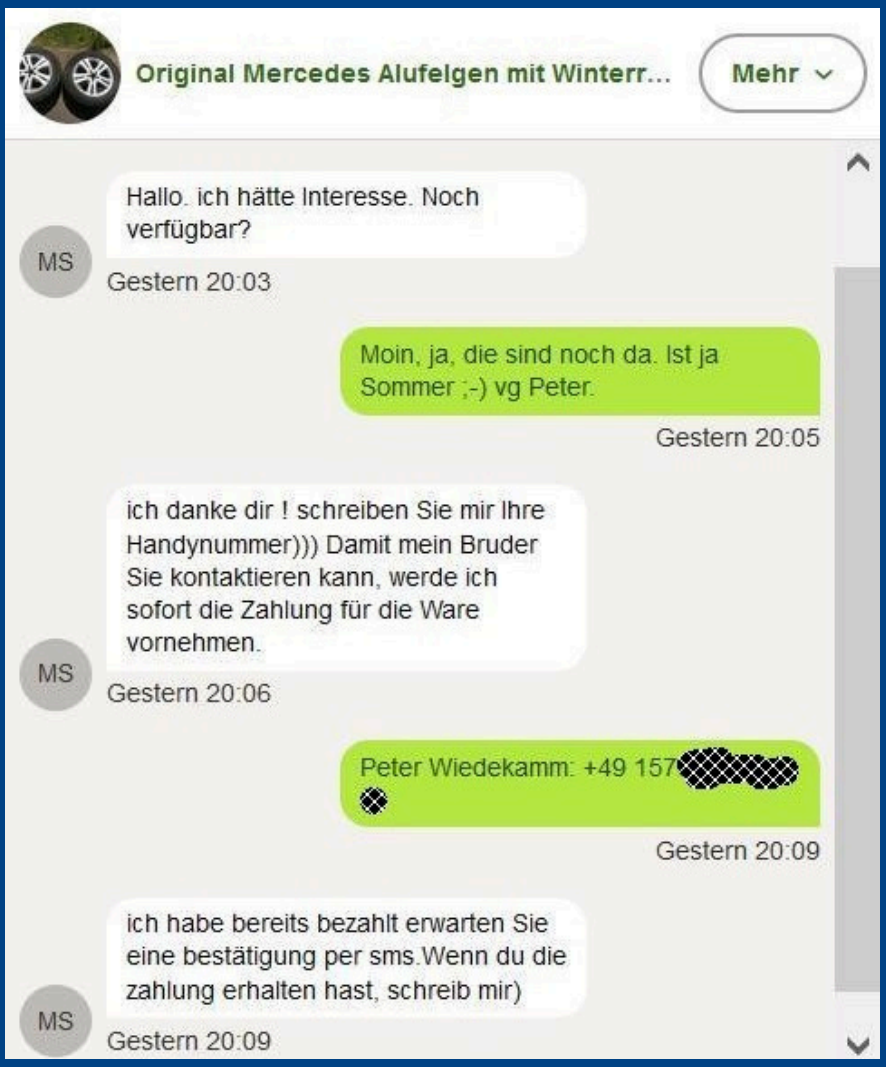
Du suchst nach einem guten Angebot bei einem online Gebrauchtwarenhändler.
Jetzt findest du ein großartiges Angebot.
Du schreibst den Verkäufer über die Plattform an. ...

3. ONLINE BETRUG: BEISPIEL

Die Verhandlungen laufen gut und ihr habt eure Mailadressen ausgetauscht und kommuniziert jetzt so, da ihr beide der Meinung wart man sehe die Benachrichtigung von dem Händler nicht zuverlässig.
Der Verkäufer ist nett und entgegenkommend, du sendest ihm einen Gutschein, da er gerade Probleme mit seinem Konto hat, er sagt, er braucht deshalb Geld und daher auch das günstige Angebot. Außerdem versichert er dir einen schnellen Versand.
Zufrieden wartest du auf dein Paket.
Das Paket kommt nicht an und der Verkäufer meldet sich nicht mehr. Die Gutscheine kannst du jetzt nicht mehr stornieren oder einlösen.
Die Händlerplattform kann dir auch nicht helfen, schließlich haben sie keine Kenntnisse vom Kauf, da du mit dem Betrüger über Mail kommuniziert hast.

3. ONLINE BETRUG: BEISPIEL

3. Beispiel:



Hier sieht man einen Verlauf von einem Verkauf bei Ebay. Beachte die Sprache und den Versuch, nicht mehr über Ebay zu verhandeln, dies sind eindeutige Hinweise auf einen Betrüger.

3. ONLINE BETRUG: ERKENNEN

Achte bei der Wahl deines online Handels auf die Bewertungen des Händlers. Wenn viele Bewertungen gegeben sind, bedeutet das viele Käufer. Aber Vorsicht, die Bewertungen können falsch sein. Wir empfehlen dir achtet auf Bewertungen von zum Beispiel Trustpilot, denn dabei handelt es sich um eine große externe Bewertungsplattform. Bei den Bewertungen empfiehlt es sich logischerweise auch auf den Ausfall dieser zu achten, extrem negative und viele Bewertungen, machen einen online Handel nicht vertrauenswürdig.
Beim Kauf gerade bei Gebrauchtwarenhändlern sollte man zudem auf die Zahlungsart achten, du solltest das Zahlen in Gutscheinen vermeiden, denn das ist extrem schwer nachvollziehbar.
Deshalb zahle lieber mit einer Überweisung . ..

3. ONLINE BETRUG: ERKENNEN

Zusätzlich solltest du es vermeiden bei Gebrauchtwarenhändlern im voraus zu bezahlen, denn der Verkäufer kann dein Geld einfach behalten, ohne dir eine Gegenleistung zu bieten. Etwas anderes wäre es, wenn du den Verkäufer persönlich oder von mehreren vorherigen Käufen kennst und dieser stets zuverlässig war.
Zur Sicherheit solltest du außerdem mit dem Verkäufer über die Gebrauchtwaren Plattform schreiben, denn dort gibt es oft Sicherheitssysteme und außerdem hasst du Nachweise auf den Betrug. ...

3. ONLINE BETRUG: ERKENNEN

Wenn du Nachrichten von starken Angeboten oder seltenen Produkten erhältst, solltet du vorsichtig sein.
Die Links in solchen Nachrichten können Viren beinhalten und dich auch auf falsche Websites schicken. Diese sind zum Teil nachbauten großer Bekannter Websites und schwierig zu enttarnen, achte auf den Website-Namen und gehe Vorsichtig mit deinen Passwörtern und besonders deinen Kontodetails um.

3.TELEFONBETRUG: DEFINITION

Als Telefonbetrug definieren wir Betrug, welcher über das Telefon begangen wird. Dabei werden die Opfer abgefragt oder in Drucksituationen gebracht.
Aber auch mögliche Millionen gewinne werden verkündet. Das Ziel der Betrüger sind deine Daten und dein Geld. Meist wird dann dein Geld von Mittelsmännern abgeholt oder auf Konten im Ausland überwiesen. Oft geben die Betrüger sich als jemand anderen aus, jemanden, den du kennst oder vertraust, wie deiner Familie oder der Polizei. Dabei nutzten sie deine Emotionen gegenüber diesen Leuten aus, um deine Wachsamkeit zu schwächen und mehr von dir verlangen zu können.

3. TELEFONBETRUG: BEISPIEL

1. Beispiel:

Du wirst angerufen. Es ist ein Rechtsanwalt, er sagt dir, du hast bei einem Gewinnspiel im Internet gewonnen, bei welchem jeder Besucher einer Website automatisch teilnimmt. Jetzt musst du ihm nur noch die Steuern für den Gewinn zahlen und du bekommst einen hohen Geldbetrag.
Glücklich gibst du dem Betrüger das Geld, er sagt, er meldet sich.
Du bekommst den Gewinn nicht.
Teilweise melden die Betrüger Gruppen sich wieder, dann eine andere Person am Telefon und teilen einen mit man hätte sich mit der Zahlung strafbar gemacht. Um nun nicht in Gewahrsam zu kommen, musst du eine Kaution zahlen oder direkt eine Geldstrafe. Mit Sorge, du hättest rechtliche Probleme, zahlst du und wurdest doppelt betrogen.

3. TELEFONBETRUG: BEISPIEL

2. Beispiel:

Der Bereich der Schockanrufe, wie der allgemein bekannte Enkeltrick.
Bei welchem dein angeblicher Enkel Schwierigkeiten hat und schnell eine Geldsumme bracht. Aus Sorge, zahlt man und denkt, man konnte das schlimmste abwenden und dann erfährt man, es war nur eine Lüge.
Hier wird dein Vertrauen und deine Bereitschaft gegenüber deinem Bekannten ausgenutzt.

3. TELEFONBETRUG: ERKENNEN

Sei vorsichtig, gerade bei hohen Geld- und Sachwerten. Bei einem möglichen Millionengewinn ruhig zu bleiben und kritisch gegenüber Zahlungen zu sein, kann dir viel Geld sparen.
Wenn die Betrüger sich als bekannte von dir ausgeben und es um einen hohen Wert geht, sei vorsichtig und versuche die betroffene Person zur Sicherheit zu kontaktieren. Wir empfehlen dir, spreche mit Familie und Freunden ein Codewort ab, welches im Fall von einem möglichen Betrug ausgetauscht werden kann. ...

3. TELEFONBETRUG: ERKENNEN

Bei zweifel frage am Anfang des Gespräches, um wen es sich handelt, wenn nur „dein Kind" als Antwort kommt, frage nach zufälligen Namen, ausgeschlossen den Namen deines Kindes, zum Beispiel: „ Michael oder Rebecca?" und deine Kinder heißen Frank, Brigitte und Hans.
Sollte der Anrufer verwundert sein und einen Namen sagen und dieser ist richtig, kannst du mit gutem Gewissen telefonieren, andernfalls lege auf oder kontaktiere die Polizei, damit möglicherweise Täter gefunden und zur Rechenschaft gezogen werden können. ...

3. TELEFONBETRUG: ERKENNEN

Sollte eine Person am Telefon dir Fragen stellen, antworte in ganzen Sätzen zum Beispiel:
Der Anrufer fragt: „Hören sie mich?”, antworte: „Ich kann sie hören.” und nicht einfach „Ja”.
Denn das Telefonat könnte aufgezeichnet werden und im Nachhinein könnten es überspielt werden.
Dann stimmst du vielleicht, ohne es zu wissen, einem Kauf zu.
Außerdem solltest du möglichst wenig persönliche Informationen preisgeben, vermeide zu sagen, wann du aus dem Haus bist, denn dies könnte für Diebstähle genutzt werden.

3. KI BETRUG: DEFINITION

Da diese Betrugsart relativ neu ist, gibt es keine klare, allgemeine Definition.
Als KI Betrug definiert ist jedoch offensichtlich Betrug mit der Unterstützung von künstlicher Intelligenz. Das beinhaltet generierte Texte, Mails, Videos, Audios oder Bilder, welche dazu genutzt werden, das Opfer zu täuschen.
Da die verbundenen Betrugsmaschen noch relativ neu sind, ist die Gefahr aktuell so groß wie nie wieder, da viele das Risiko des Betrugs unterschätzen. Die größte Gefahr geht dabei von den echt aussehenden Bildern und Videos sowie nachgemachten Stimmen beispielsweise am Telefon aus.
Sogenannte Schockanrufe versuchen teilweise mit durch KI geklonten Stimmen von bekannten Stresssituationen zu erzeugen, damit das Opfer nicht mehr rational denkt.

3. KI BETRUG: NEUE GEFAHR

Denn selbst Berlins ehemalige Bürgermeisterin Franziska Giffey ist auf einen KI-Betrug hereingefallen: Sie hat in einer Videokonferenz mit einer Deepfakeversion von Klitschko (Bürgermeister von Kiew) gesprochen.

Videokonferenz Fälschung

Original

3. KI BETRUG: NEUE GEFAHR

Ein Beispiel eines Sogenannten “Deepfakes”

Bei diesem Deepfake von Obama, ist kaum bis gar nicht erkennbar, dass es sich um eine Fälschung handelt. Das linke Bild ist könnte auch ein Foto sein, so wie das Rechte. Der einzige erkennbare Unterschied ist bei den Augenbrauen.

3. KI BETRUG: BEISPIEL

1. Beispiel:

Bei den vorher genannten Schockanrufen handelt es sich um eine alte Masche, nach dem Prinzip des bekannten Enkeltricks.
Mit der Entwicklung der KI gibt es aber eine ganz neue und stärkere Gefahr. Betrüger rufen gezielt deinen Enkel an und möchten eine Umfrage machen, durch das Gespräch kann mithilfe von KI die Stimme deines Enkels nachgemacht werden. Nun rufen die Betrüger dich an und können in der Stimme deines Enkels, auch mit verschieden Emotionen sprechen. Oft kommt dann etwas wie: „Ich habe einen Unfall gebaut und brauche schnell Geld um nicht ins Gefängnis zu kommen.“ dabei spielen die Betrüger mit deinen Emotionen und du zahlst, da schließlich dein Enkel selbst mit dir gesprochen hat und nicht irgendwer anders, deshalb denkst du, dass es kein Betrug sein kann.

3. KI BETRUG: BEISPIEL

2. Beispiel:

Auch bei Videos kann das Aussehen in einem Videoanruf verändert werden, da viele Videos von sich auf den sozialen Medien teilen, kann es daher wie bei der ehemaligen Berliner Bürgermeistern zu falschen Videoanrufen oder Videos kommen. Damit sollte man Vorsichtig sollte sein, denn so kann jedem jedes Wort in den Mund gelegt werden und Straftaten wie Verleumdung vereinfacht werden.
Außerdem besteht eine Gefahr, denn wenn du sicher gehen möchtest, dass du am Telefon die richtige Person hast und einen Videoanruf startest, kann auch dieser Teil des Betrugs sein.

3. KI BETRUG: ERKENNEN

Das Erkennen von KI Fälschungen ist meistens schwer. Oft gibt es ersichtliche Fehler bei Bildern und Videos. Die Mimik und Gestik wirkt unnatürlich oder Körperteile sind zu oft da, zum Beispiel sechs Finger. In der Regel ist auch die Qualität der Videos schlecht, klare Verpixelungen sind zu erkennen. Gerade da dies bei manchen Videokonferenzbetreibern häufig ist, kann man leicht auf die Fälschungen hereinfallen. Sollten mutmaßlich deine Bekannten betroffen sein, kontaktiere diese, um sicherzustellen, dass sie es tatsächlich sind. Hier raten wir ein gemeinsames Codewort mit bekannten festzulegen, gerade wenn es um Geld geht, ist Sicherheit wichtig. Außerdem solltest du aufpassen, was du im Internet öffentlich teilst, damit es den Betrügern nicht einfacher gemacht wird deine Bekannten zu betrügen.

4. FAZIT

Es ist kompliziert und gerade durch KI gibt es neue Betrugsmaschen, welche extrem schwer zu erkennen sind. Um nicht auf die Verschiedenen aktuellen Betrugsmaschen: Phishing, Online, Telefon und KI Betrug hereinzufallen, muss man aufmerksam bleiben und bei Kontaktaufnahme, welche Angaben und/oder Zahlungen angegeben haben möchte kritisch bleiben. Bei dem Versuch dich mithilfe von Emotionen zu nötigen musst du versuchen rational zu bleiben.

DU HAST NOCH FRAGEN ODER KRITIK?
MELDE DICH GERNE BEI UNS!

digital impact lab

MAIL: LINDEMANN@M2C-BREMEN.DE
TEL: +49 176 57880024
WEB: IMPACT-LAB.EU/SPI

Unsere Unterstützer:

HAPNET

Freie Hansestadt Bremen

Co-funded by the European Union

M 2 C