Schutzbuch Internet-Betrug

Trolljäger. Von wegen nettes, altes Opfer

Sprechstunde 1: Worin besteht die Gefahr?

Verfasser: Timmo Strohm / Version 1.0

Erscheinungsdatum: 7.7.2025

Worin besteht die Gefahr?

Sorgen sind nur schlecht organisierte Pläne

Zur Sprache #inklusion

Beachten Sie bitte unseren Inklusions-Hinweis am Ende des Dokuments. Grundsätzlich wendet sich dieser Text respektvoll an alle und jede/n ohne irgendjemand auszuschließen.[1]

Kurzfassung

Durch Internet-Betrug und Telefonbetrug drohen extreme Schäden. Als Gegenwehr bleibt uns nur Vermeidung durch Wachsamkeit, Prüfung und Kontrolle. Entgehen kann man dieser Automatik nicht, sie ist Bestandteil der globalisierten Kommunikationstechnik, die wir als Telefon im Haus haben und als "Handy" mit uns herumtragen

Wie heißt das Phänomen eigentlich? #worumgehtes

Verbrechen per Telefon oder Internet gelten als "Cybercrime". Eines der häufigsten Probleme, der Online-Betrug, ist aber einfach ein gewöhnlicher Betrug, der eben per Telefon oder "Social Media" stattfindet. Er wird daher auch als Betrug verfolgt.

Der gefährliche Unterschied ist leider die Reichweite, weil *online* ein und derselbe Betrug viele tausend Opfer gleichzeitig betreffen kann. Man merkt, dass schon hier ein "normaler" Betrugsermittler, der gewöhnlich mit wenigen Opfern eines Täters zu tun hat, überfordert

sein könnte - und dasselbe gilt für die Prävention.

Wir reden in diesem Schutzbuch pauschal von **Internet-Kriminalität**, da alle Begehungsformen erst durchs Internet ermöglicht wurden und im Internet stattfinden. Die Täter schlagen aus weiter Entfernung zu, ohne Risiko, anonym und in der Sicherheit, niemals gefasst oder bestraft zu werden.

Die Grunddelikte sind seit Jahrtausenden gleich: Betrug, Raub, Diebstahl, Unterschlagung, Erpressung, Entführung oder Körperverletzung.

Trügerisches Sicherheitsgefühl

Weil wir dem Internet nicht in nachtdunklen Seitenstraßen begegnen, sondern in der Sicherheit unserer Wohnküche oder unseres Kinderzimmers, haben wir schon den ersten Nachteil: die Schurken haben die Überraschung auf ihrer Seite. Wir ERWARTEN einfach keinen Überfall im Flur oder in der Speisekammer. *My home is my castle.* Zuhaus fühlen wir uns unangreifbar, selbst die Polizei darf da nicht ohne Erlaubnis rein.

Genau das ist auch das Problem für Leute, die warnen wollen: die Armee der Warner, die Soldaten der Prävention. "Ich hab doch keinem was getan", denken die zukünftigen Opfer. "Wer sollte schon auf mich losgehen wollen", "ich hab nichts zu verbergen", "ich bin ja nicht reich" - kurz: Was will man von mir?

Dleses erste Kapitel beantwortet genau das.

Wer sind die Gegner?

Viele Menschen meinen, dass das Problem sie nicht betrifft. Unsere Feinde und Gegner sind in diesem Spiel aber leider nicht nur raffinierte Mafiosi in fernen Landen, sondern auch Politiker, Anwälte und oft genug unser Umfeld: Menschen, die der Mafia helfen. Sie unterstützen die Bösartigen durch totale Missachtung des Opferschutzes. Die Justiz bleibt untätig, der Politiker kennt nicht einmal das Problem, die Gesellschaft höhnt und spottet. Journalisten berichten über das Phänomen mitleidig und herablassend und nicht selten in einer Sprache, die von Anfang an so exklusiv wie überhaupt nur möglich ist. Dabei nutzen

und erfinden viele Zeitungsleute, um fachlich versiert zu klingen, Pseudo-Fachsprache aus Abkürzungen oder Kofferworten ("Quishing").

Die Täterinnen und Täter sind teils ganz einfach Programme und Automatenstimmen. Die Menschen sind leider meist höchst durchorganisierte Gruppen oder Schattenfirmen. Häufig sitzen sie in der Türkei oder Pakistan, häufig sind auch Angriffe aus Indien, China und Russland dabei. Manche sind geradezu bürgerlich organisiert und bieten ihrem Telefonpersonal feste Gehälter. Es gibt auch Sklaverei-Betriebe, deren Insassen mit Essensentzug gequält werden, wenn sie keine Betrugserfolge vorweisen können. Der deutschen Strafjustiz sind diese Strukturen in jedem Falle unzugänglich.

Auf der Seite der Opfer sind nur die, die beruflich Prävention betreiben - sowie ein paar Fachleute oder Interessierte, die sich mit dem Problem befassen, so wie Sie selbst jetzt gerade. Für viele normale und freundliche Menschen wie Sie und mich ist aber das Hauptproblem, dass wir uns die innere Haltung der Angreifer - das Scammer Mindset - einfach nicht vorstellen können. Wir haben es nicht nur mit modernster und hochgerüsteter Technik zu tun, sondern auch mit Menschen, die heuchlerisch freundlich und verständnisvoll klingen. Es sind Stimmen die sich scheinbar herzlich mit uns unterhalten, zuhören, Verständnis äußern, auf uns eingehen - und uns gleichzeitig finanziell für ewig ruinieren, uns schweren seelischen und sozialen Schaden zufügen, und das einfach nur, weil das so leicht und straflos möglich ist.

Was kann überhaupt passieren - schlimmstenfalls?

Bestes Mittel gegen Angst ist Genauigkeit. Worum geht es überhaupt? Schließlich ist es ein Unterschied, ob mir nur ein kleiner Geldverlust oder die Vernichtung meiner Existenz droht. Und - kann "das Internet" wirklich so schrecklich sein? Die gefährlichsten Schäden sind finanzielle, soziale, höchstpersönliche und datenbezogene. Denken Sie an den maximalen Schaden, den ein Mensch sich selbst zufügen kann: Totale Zerstörung der bürgerlichen Existenz, Verschuldung, Kriminalität, Körperverletzung bis hin zum Selbstmord. Manipulatoren wollen uns zu maximaler Selbstschädigung verleiten.

Es droht ungeheuerliche und *unvorstellbare* Gefahr in folgenden Bereichen:

Finanziell

Schwerer Vermögensschaden bis hin zur Existenzvernichtung

Verschuldung, ebenfalls bis hin zur Existenzvernichtung

Soziales Umfeld

- Zerstörung von Beziehungen, teils irreparabel
- Arbeitsplatzverlust, bis hin zur totalen Unvermittelbarkeit
- Rufschaden, bis hin zum totalen Ausgestoßenwerden aus der Gemeinschaft

Freiheit und körperliche Unversehrtheit

- Entführung, bis hin zum Ausgeliefertsein an Menschenhändler
- Körperverletzung, auch schwere
- Sexueller Missbrauch, bis hin zum Ende in der Sexualsklaverei und erzwungener Drogenabhängigkeit
- Bei Minderjährigen und leicht Beeinflussbaren: Manipulation zur Selbstverletzung / Gefährdung

Informationsfreiheit, Privatheit

- Datenverlust, bis hin zum Totalverlust ganzer Firmen
- Sabotage: Beschädigung / Totalausfall des Computers oder Netzwerks
- Spionage: Datendiebstahl, Datenmissbrauch, Identitätsdiebstahl
- Zweckentfremdung des Computers (Botnetz-Viren, Crypto-Miner)

Gesellschaftlich

Online Betrüger ("Scammer") zerstören das gesellschaftliche Grundvertrauen. Der Gesellschaftsvertrag besteht in der Akzeptanz gemeinsamer Normen. Vertrag heißt, dass wir uns vertragen, einander nicht permanent Fallen stellen, belügen, täuschen und

versuchen, uns gegenseitig so übel wie möglich zu schädigen. Wir können nicht von jedem Polizisten Ausweis und Dienstnummer verlangen und mit seinem Vorgesetzten telefonieren, bevor wir auf sein Haltezeichen reagieren. Auf amtliche Anweisungen im Katastrophenfall müssen wir reagieren, ohne vorher zu fragen, ob da auch wirklich ein Erdrutsch droht oder nur Schurken uns kurz aus dem Haus treiben wollen, um es in Ruhe auszuräumen. Behörden, Banken und Firmen haben kaum noch Möglichkeiten, reibungslos mit der Bevölkerung zu kommunizieren - und sie werden durch eine Flut unnötiger Nachfragen gelähmt. Außerdem müssen sie ständig vor dem jeweils aktuellen Missbrauch ihrer Namen, Adressen und Symbole warnen.

Wie geht das? Angriffsmethoden

Verbrecher manipulieren uns, ihre Opfer, **technisch** und **psychologisch**. Sie verfügen in beiden Bereichen über überlegene Mittel, über geheimdienstliche, militärische und psychologische Ausbildung. Sie setzen ganze Gruppen von Technikern, Psychologen und Soziologen ein, unterstützt von Fälschern, Schauspielern und neuester Technologie. Außerdem sind sie durch Datendiebstähle und Recherche vorbereitet und wissen oft vieles über ihre Opfer, von dem diese nicht ahnen, dass Fremde oder gar Verbrecher an diese Information gelangen können.

Die Gangster sind vollkommen skrupellos, hoch aggressiv, kennen weder Gnade noch Verständnis noch Rücksicht und betrachten ihre Opfer als Schlachtvieh. Nicht ohne Grund heißt eine der meist-verbreiteten Betrugsmaschen "**Schweineschlachtung**" ("*pig butchering scam*").

Die Annahme, Durchschnittsbürger könnten sich gegen so etwas erfolgreich verteidigen, zeugt von totaler Ignoranz dem Thema gegenüber und fachlich von geradezu barbarischer Inkompetenz.

Durch Training und ein Bündel von Maßnahmen kann die Situation verbessert werden. Die Chancen können erhöht werden, dem Angriff zu entgehen oder wenigstens den Schaden zu begrenzen.

DAS ist das Anliegen dieser Reihe von Schriften und Videos.

Technisch nutzen die Kriminellen:

- Computerviren und Malware
- SEO (Suchmaschinen-Beeinflussung)
- Internet-Technik: Spam und Massenmails, Roboterprogramme, Hacking, Fälschung des Absenders oder der Herkunftsnummer ("*Spoofing*")[2]
- Fälschung (Fake News, *Deep Fakes*, Desinformation)
- All das verstärkt, beschleunigt und ins Unendliche gesteigert durch "KI", also "Künstliche Intelligenz"

Psychologisch nutzen die Kriminellen jede nur denkbare Methode der Manipulation: Schock, Drohung, Versprechen, Heiratsschwindel oder Liebes-Täuschung, Gewinnversprechen, Religions-Missbrauch, Vorgetäuschte Notlage eines Angehörigen, Vorgetäuschte Notlage Fremder, Angstmachen, Erwecken von Habgier oder sexueller Gier, Amtsanmaßung, kurz - jede nur denkbare Form der Täuschung und der Lüge. Sie arbeiten mit Drohung, Versprechen, Amtsanmaßung, Emotionaler Erpressung, Einschüchterung, Irreführung - wobei **alles** Desinformation ist, denn das Ganze ist unreal und würde uns, wenn wir das von Beginn an wüssten, nicht mehr beeindrucken als eine

dumme Fernsehwerbung oder ein noch dümmerer Horrorfilm.

Ziel ist ausnahmslos, einen Irrtum zu erwecken, der das Opfer zu einer Handlung veranlasst, die dem Täter in irgendeiner Form Nutzen bringt: Täuschung führt zu Irrtum, Irrtum führt zu einer Verfügung (über Geld, Wertgegenstände, Information, Zugang zu Räumen oder Daten...). Der Verlust an Wert, Sicherheit oder Geheimnisschutz, der dadurch entsteht, ist der Schaden - was abstrakt klingt, wird entsetzlich greifbar, wenn tatsächlich Ihr Vermögen weg ist oder Ihr Haus gepfändet wird.

DIE GEFAHR IST ZUGLEICH DIE RETTUNG: OHNE IHRE MITHILFE GEHT ES NICHT

Gefahr konkretisiert

Weil das Opfer "mitwirken" muss, also zu etwas verleitet wird, kann es den Angriff verhindern. Theoretisch.

Im Einzelnen nenne ich die wichtigsten Angriffsmethoden und die entsprechende Schutzmaßnahme

1. Technisch

Angriffsmethode oder -werkzeug	Gegenmittel
ComputerViren	Antivirus Software Empfehlenswert sind deutsche Hersteller von Antivirus-Software aus Gründen des Rechtsschutzes und der

Angriffsmethode oder -werkzeug	Gegenmittel
	Privatheit. Strohm IT empfiehlt GData aufgrund eigener langjähriger Erfahrung - gute Hotline, guter Service und immer wieder Testsieger bei Fachzeitschriften und bei der Stiftung Warentest Sie benötigen eine *kostenpflichtige* Antivirus Software.
Malware[3]: Schadprogramme Scareware NagScreens RootKits RansomWare	Wie Viren; zusätzlich sollten Sie nur Programme installieren, ohne die es einfach nicht geht. Auf keinen Fall sollten Sie Programme "zum Ausprobieren" installieren oder solche, die Spiele oder Witze enthalten. Sie müssen wissen, was Sie tun - und warum. Zum Lernen oder Herumspielen können Sie ein altes Handy oder Wegwerfgerät nutzen, dessen Totalausfall Ihnen gleichgültig ist. Faustregel: Installier nur Programme, ohne die es nicht geht Die meiste MalWare ist ein vermeidbarer Unfall. Spiele, Sinnlos-Apps und Müllsoftware mit reißerischen Versprechungen sind hier die Hauptquelle. Wenn Sie ein Programm auf Ihrer wichtigsten Informationsquelle UND Ihrem wichtigsten Kommunikationsmittel installieren, müssen zwei Bedingungen zwingend und unbedingt erfüllt sein: 1.) Sie wissen genau, was Sie da tun, warum Sie es tun und von wem das Zeug kommt 2.) Genau diese Software ist unverzichtbar, es geht

Angriffsmethode oder -werkzeug	Gegenmittel
	einfach nicht ohne sie
SPAM[4]	Spamfilter - und das Wegschauen und Nichtbeachten

2. Psychologisch: Schock-Anrufe

Telefonbetrug kommt in zahllosen Maschen daher. Sie versprechen, drohen, täuschen.

AUFREGUNG ist eine Warnlampe. Anrufe aus dem Nichts, die aufregend sind, sind so gut wie immer Fälschungen.

UNWAHRSCHEINLICHKEIT ist ein weiteres Warnsignal. Wenn Banken, Geheimdienste, Kriminalpolizisten und Software-Konzerne bei uns anrufen, um für uns unentgeltlich zu arbeiten oder sich ohne jeden Auftrag um unsere Belange zu kümmern, muss uns klar sein, dass das einfach nicht sein kann. Wer arbeitet schon umsonst?

Betrügerische Angebote sind ebenfalls ein Warnsignal, fallen aber in die Schublade "Aufregung" - denn natürlich sind wir über das Angebot ganz aus dem Häuschen, das einfach zu schön ist, um wahr zu sein. Nichts Gutes rennt uns nach. Nichts Gutes macht Werbung in Schmuddelforen. Geheimtipps werden nicht öffentlich im Internet beschrieen und gute Börsen-Anlagen sind auch nichts mehr wert, wenn sie dann per E-Mail an die letzten 800 Millionen Provinz-Haushalte geschickt wurden.

Hier hilft einfach nur Vernunft, Informiert-sein und Nachforschen.

Die Regeln sind:

Geldanlage - Nicht ohne Besprechung

Abzocke - Nichts ohne Nachfrage; Kenne Deine Rechte; lege eine Vertragspartner-Liste an.

Drohung - Sofort rückfragen und sofort auflegen, wenn die Gegenstelle meint, Rückfragen seien aus irgendwelchen Gründen nicht möglich oder verboten.

Die Macht der Recherche ist generell die einfachste und schnellste Abhilfe. Es genügt meist schon, nur die wesentlichen Stichworte der "Masche" einzugeben, um darauf zu stoßen, dass es eine Betrugsmasche ist.

Vorteilhafte Angebote laufen uns nicht nach und kommen auch nicht per Telefon, weshalb wir an Angeboten, die uns per Anruf ins Haus schneien, generell nicht interessiert sind - es SIND Betrugsangebote.

Gefährliche Irrtümer und die richtige Antwort

Irrtum	Realistischer Abgleich
Dies auszuprobieren, könnte Ihnen nützen oder Spaß machen	Brauche ich das - geht es nicht auch ohne das?
Dies könnten Sie billig kaufen	Gib es das gratis?
Das passiert mir ja nicht	Doch, die Automatik erwischt jeden tausendfach, sie schickt Millionen Nachrichten pro Tag an alles und jeden
Ich habe nichts zu verbergen	Doch, weil man Ihre Daten missbraucht und Ihre Identität stiehlt - der Ärger bleibt an Ihnen hängen
Für mich interessiert sich niemand	Doch: Krankenkassen, Politische Akteure, Versicherungen, Datenhändler, Abzocker, Mafia auf Opfersuche, Entführer, Organhändler...

Irrtum	Realistischer Abgleich
Ich bin ja nicht bedeutend	Jemand, den Sie kennen und der bedeutend ist, ist das Ziel
Ich falle auf so etwas nicht rein	Jeder und jede ist verwundbar
Die Opfer sind selber schuld	... diese Idee hilft den Tätern, gekauften Politikern, der bequemen Justiz, den Gehässigen und Denkfaulen, der Mafia und ihren Lobbies. Vor allem schadet diese Idee IHNEN. Denn Sie könnten die oder der Nächste sein

Online-Sprechstunde live:

Timmo Strohm lädt Sie zu einem geplanten Zoom-Meeting ein.

Thema: Sicherheit im Internet: Online-Sprechstunde
Zeit: 11.Juli 2025 09:00 AM Amsterdam, Berlin, Rom, Stockholm, Wien

An Zoom-Meeting teilnehmen
https://us04web.zoom.us/j/75689485196?pwd=OHv2MgKSCwRiov6VlmkKQl5LR126iB.1

Meeting-ID: 756 8948 5196
Kenncode: 2L92Ag

Jede Woche am Freitag von 9:00 Uhr bis 9:30 Uhr

Bitte laden Sie die folgenden iCalendar (.ics)-Dateien auf Ihr Kalendersystem herunter und importieren Sie sie.

Wöchentlich: https://us04web.zoom.us/meeting/upErf-Cspj4rE9Jgtq2WwD8v1ABTZ-slPXmv/ics?icsToken=DJ61Ql5qS-tu8VUEMAAALAAAAIQpz2E9Ul0sfWZGtdQ9B-tQZpPI4EgHPneDym8hGzCgdAtR3B-1NCB62836uU9K898nvLP3PlxR6p-xyTAwMDAwMQ&meetingMasterEventId=idGtxZZrQsyo7Q52OMVgog

Impressum

Verantwortlich für diese Publikation:

Timmo Strohm

strohm.IT

Adresse:

Broner Platz 3

88250 Weingarten

Telefon: 0751 / 5681 - 3924

Mobil: 0174 - 9607 150

E-Mail: info <at> strohm.it

Internet: https://www.strohm.it

Inhaltlich Verantwortlicher gemäß § 55 Abs. 2 RStV / V.i.S.d.P.:

Timmo Strohm (Anschrift wie oben)

Das Unternehmen Strohm IT befasst sich mit Online Publikation.

1 Plurale und Gendern: In diesem Dokument sind grundsätzlich Menschen ALLER denkbaren Gruppen oder Identitäten gemeint, wenn von Gruppen die Rede ist (mit "der Betrüger" ist auch "Betrügerin" gemeint, mit "Verbrecher" auch "Verbrecherinnen"). Aus Rücksicht auf Menschen, die Übersetzungshilfen, Lesehilfen, Vorleseprogramme und anderes einsetzen müssen sowie aus Rücksicht auf Menschen mit Verständnis-Schwierigkeiten setzt dieser Text ungegenderte Standardsprache ein, die leicht mit Automatik zu filtern, zusammenzufassen oder zu verarbeiten ist.

2 Spoofing bedeutet, in einer E-Mail, einem Telefonprogramm oder anderen Komunikationsformen zu verschleiern oder zu fälschen, wer die Nachricht in Wirklichkeit absendet. Dadurch glauben die Empfänger zum Beispiel, ein Anruf käme von einem Verwandten oder Freund, während sie in Wirklichkeit mit einem Verbrecher sprechen, der auch noch die Anruferstimme fälscht.

3 Malware sind unerwünschte und ohne Erlaubnis des Computer-Eigentümers installierte Programme. Häufig werden sie unter falschem Namen, getarnt oder heimlich im Hintergrund des Betriebssystems installiert. Unterarten sind: "Scareware", also Programme, die uns mit Drohungen unter Druck setzen; NagScreens, also störende Fenster, die immer wieder erscheinen; RootKits, die sich tief im Betriebssystem einnisten und Computer lahmlegen können; und RansomWare, also Erpresserprogramme, die mit Schäden oder Datenverlust drohen, falls nicht gezahlt wird.

4 "SPAM" ist ganz ursprünglich ein Kofferwort, eine Zusammensetzung aus "Spiced" und "Ham". Im Internet-Jargon steht das Wort für maschinell erzeugtes Füllmaterial, das in alle denkbaren Informations-Container gefüllt wird, ähnlich wie der Fleischbrei in "Spam" Konserven.