fundstück

2/2026 | Beilage der Norddeutschen Hausbesitzer Zeitung



ÖRAG
Cyber-Rechtsschutz exklusiv für Haus & Grund-Mitglieder
(S. 11)

Verbrechen im Netz

Schutz für Haus & Grund-Mitglieder

STADTWERKE KIEL 24/7

HORIZONT GAS:

GÜNSTIGER ALS GEDACHT

Weitblick zahlt sich aus. Auch beim Gastarif.

Wechseln Sie jetzt unter Angabe des Aktionscode „**Gas247**“
und kommen Sie gut vorbereitet durch die kalte Jahreszeit.

Jetzt online wechseln auf:
stadtwerke-kiel.de/gasangebot

Jetzt wechseln und sparen!

Frische Energie für die Zukunft.

Preise variieren je nach Wohnort – siehe Online-Tarifrechner. Dort finden Sie auch die Vertragsbedingungen (AGB). Mindestvertragslaufzeit 12 Monate, danach monatlich kündbar.

Verbrechen im Netz

INHALT



Das Ziel ist der Mensch, nicht die Technik 4
Maßnahmen 8
Wir wollen oft glauben, was wir hoffen 10
Cyber-Rechtsschutz 11
Was passiert mit den Opfern, wenn die Polizei gegangen ist? 12
Tipps 15
Stoppen.Hinterfragen. Schützen. 16
Der Trick an der Haustür 18

Liebe Leserinnen und Leser,

das Internet und mit ihm all seine Leistungen wie Soziale Medien, das Online-Shopping, das Buchen von Hotels oder Reisen oder das Online-Banking sind Errungenschaften unserer Zeit, die wir uns aus unserem täglichen Leben nicht mehr wegzudenken vermögen. Sie verbinden uns mit anderen Menschen und erleichtern uns den Alltag in vielerlei Hinsicht. Doch wie heißt es so schön: Wo viel Licht ist, ist auch Schatten. Längst haben sich kriminelle Strukturen etabliert, die vor allem im Bereich des Betrugs im weltweiten Netz ihr Unwesen treiben und die Nutzer desselben um eins ihrer liebsten Güter, ihr Geld, zu erleichtern versuchen. Wir haben mit „Verbrechen im Netz“ für Sie diesmal eine Ausgabe des Fundstücks zusammengestellt, in der wir über diese Risiken und Gefahren aufklären möchten und Ihnen gleichzeitig Tipps und Informationen an die Hand geben wollen, wie Sie ihnen begegnen und sich schützen können. Bleiben Sie aufmerksam und vorsichtig.

Eine erkenntnisreiche
Lektüre wünschen Ihnen

Sönke Bergemann — Dr. Philipp Pries

IMPRESSUM

Eine Beilage der
Norddeutschen Hausbesitzer Zeitung

HERAUSGEBER
Haus & Grund Kiel, Haus-, Wohnungs- und Grundeigentümerverein von Kiel und Umgegend e.V.

VORSITZENDER:
Götz Bormann

GESCHÄFTSFÜHRER:
Sönke Bergemann

Sophienblatt 3, 24103 Kiel
Telefon: 0431 66 36 123,
Telefax: 0431 66 36 180
info@haus-und-grund-kiel.de
www.hausundgrund.de/verein/kiel/

Vereinsregister-Nr. 502 VR 1959,
Amtsgericht Kiel, Finanzamt Kiel

VERLAG, HERSTELLUNG, VERTRIEB
Haus & Grund Kiel –
Verlag & Service GmbH
Stresemannplatz 4, 24103 Kiel
Telefon Redaktion: 0431 66 36 218
Telefon Vertrieb: 0431 66 36 121
verlag@haus-und-grund-kiel.de
www.hausundgrund.de/verein/kiel/verlag-service

LAYOUT & GESTALTUNG
Sarah Raymann

GESCHÄFTSFÜHRER
Sönke Bergemann

REDAKTIONSLEITUNG
Dr. Philipp Pries (verantw.)

REDAKTION
Stefanie Lettau

Handelsregister
Amtsgericht Kiel HRB 11053 KI

DRUCK
PerCom Druck- u. Vertriebsgesellschaft mbH,
Am Busbahnhof 1
24784 Westerrönfeld

MEDIABERATUNG
Merle Schneider
Telefon: 01511 1 07 58 61
info@nhz-online.de

Nachdruck, auch auszugsweise, nur mit ausdrücklicher Genehmigung der Redaktion. Belegexemplare erbeten. Über unverlangt eingesandte Manuskripte und Fotos freuen wir uns sehr, wir übernehmen jedoch keine Haftung. Die Redaktion behält sich vor, eingesandte Artikel nach eigenem Ermessen zu kürzen. Hinweis: Gewerbliche Anzeigen müssen nicht bedeuten, dass darin beworbene Artikel von der Redaktion empfohlen werden. Mit dem Namen des Verfassers gekennzeichnete Beiträge stellen nicht unbedingt die Meinung der Redaktion dar.

TITELFOTO, INHALT: KI GENERIERT, ISTOCK, POLIZEILICHE KRIMINALPRÄVENTION DER LÄNDER UND DES BUNDES (LANDESKRIMINALAMT BADEN-WÜRTTEMBERG)





Das Ziel ist der Mensch, nicht die Technik

Gefahren beim Online-Banking

Immer mehr Kundinnen und Kunden von Banken und Sparkassen nutzen das Online-Banking. Es ist bequem und praktisch, Geldgeschäfte und Überweisungen von zu Hause aus erledigen zu können, ohne eine Filiale aufsuchen zu müssen. Aber wer nicht Opfer von Kriminellen werden möchte, sollte dringend grundlegende Sicherheitsregeln beachten. Auch die Bankinstitute müssen sich gegen Übergriffe von Betrügerinnen und Betrügern absichern. Einen Einblick zu aktuellen Gefahren und Maßnahmen gibt Sven Kietzke, Experte für das Electronic Banking bei der Förde Sparkasse in Kiel.

Herr Kietzke, welche Gefahrenquellen im Online-Banking sind derzeit aus Ihrer Sicht am relevantesten? Welche neuen Angriffsvektoren haben Sie im letzten Jahr im Vergleich zu vorherigen Jahren beobachtet?

Betrügerinnen und Betrüger setzen bereits seit Jahren ausschließlich auf Phishing und Social Engineering. Gefälschte Textnachrichten, gefälschte E-Mails, betrügerische Telefonanrufe – das Angriffsziel ist in den allermeisten Fällen der Mensch und nur ganz selten die Technik. Im Laufe der letzten Jahre haben die Kriminellen ihr Vorgehen dahingehend professionalisiert, dass sie inzwischen sehr überzeugend auftreten und genau wissen, wie sie ihre Opfer zu bestimmten Handlungen bewegen können.

Welche technischen und organisatorischen Sicherheitsmaßnahmen setzen Sie ein, um Konten gegen aktuelle Bedrohungen abzusichern?

Aus technischer Sicht ist unser Online-Banking mit der Zwei-Faktor-Authentisierung gut gegen aktuelle Bedrohungen aufgestellt. Gleichwohl arbeiten wir kontinuierlich an Verbesserungen wie zum Beispiel deutlicheren Warnhinweisen innerhalb unserer pushTAN-App bei besonders schutzbedürftigen Auftragsfreigaben.

Die wichtigste und für uns relevanteste Sicherheitsmaßnahme ist jedoch ganz klar die Aufklärung. Nur wer die aktuellen Gefahren kennt, kann im Fall der Fälle entsprechend reagieren. Hierzu finden unsere Kundinnen und Kunden und in unserer Internet-Filiale nicht nur umfangreiche Informationen zum Thema Sicherheit im Online-Banking, sondern auch aktuelle Warnhinweise mit Beispielen und Screenshots. Auch unsere Kolleginnen und Kollegen werden in regelmäßigen Abständen zu den aktuellen Betrugsmethoden sensibilisiert, um das Verhalten im Ernstfall zu schulen.

Welche Betrugsmaschen, wie unter anderem Phishing, Fake-SMS oder Business-Email-Compromise, stellen aktuell die größten Risiken dar, und wie unterscheiden sich diese je nach Kundensegment?

Die größte Gefahr geht heutzutage von gefälschten Textnachrichten per SMS aus, meist gefolgt von einem darauf aufbauenden betrügerischen Telefonanruf. Der Ablauf ist dabei stets gleich: Im ersten Schritt verschicken Betrügerinnen oder Betrüger eine Textnachricht mit einem Link, der zu einer gefälschten Anmeldeseite führt. Haben die Kriminellen hierüber die Zugangsdaten ihres Opfers erbeutet, rufen sie es im zweiten Schritt an, geben sich beispielweise als Bankmitarbeiterin oder Bankmitarbeiter aus und bringen ihr Opfer dazu, betrügerische Transaktionen freizugeben. Als Begründung werden dabei unter anderem angeblich abgelaufene oder aktualisierte Sicherheitsmittel genannt, die durch die Kundin beziehungsweise den Kunden neu bestätigt werden müssen. Inhaltlich variieren die Texte nur leicht und sind grundsätzlich allgemein gehalten, um möglichst viele potenzielle Opfer anzusprechen.

Woran können Kundinnen und Kunden gefälschte Bankwebseiten oder E-Mails erkennen?

Bei Webseiten genügt oft ein Blick auf die URL, also die im Browser angezeigte Adresse. Diese besteht im Betrugsfall meist aus ungewöhnlichen Zeichenkombinationen, die nur wenig mit der tatsächlichen Adresse der jeweiligen Bank gemeinsam haben. Bei E-Mails oder Textnachrichten ist insbesondere auf den Inhalt zu achten. Wird ein akuter Handlungszwang ausgesprochen und damit verbunden dazu aufgefordert, auf einen enthaltenen Link zu klicken, ist definitiv Vorsicht geboten. Noch wichtiger ist jedoch, bei eingehenden Telefonanrufen aufmerksam zu sein und sich niemals von einer fremden Person dazu verleiten zu lassen, Transaktionen im Online-Banking zu bestätigen oder wichtige Sicherheitsmittel wie zum Beispiel PIN, TAN oder Passwörter preiszugeben. Kein seriöser Bankangestellter wird je zu so etwas auffordern. ▶▶



Sven Kietzke





Welche Rolle spielen Zwei-Faktor-Authentisierung und TAN-Verfahren für die Sicherheit? Wie bewerten Sie deren Effektivität und welche Veränderungen planen Sie in Bezug auf Passwortrichtlinien oder moderne Authentifizierungsmethoden wie Passkeys?

Die Zwei-Faktor-Authentisierung ist ein äußerst effektiver Schutz. In unserer pushTAN-App werden beispielsweise bei jeder Auftragsfreigabe die Details des jeweiligen Auftrags angezeigt. Diese sollten vor der Freigabe noch einmal kontrolliert werden. Zeigt die pushTAN-App Auftragsdetails an, die von dem gewünschten Auftrag abweichen oder seltsam erscheinen, ist die Freigabe abzubrechen. Dasselbe gilt für Auftragsfreigaben, die man nicht selbst initiiert hat. Selbstverständlich beobachten wir hierbei die technischen Entwicklungen und passen unsere Sicherheitsvorkehrungen laufend an.

Was empfehlen Sie Kundinnen und Kunden, wenn sie eine verdächtige Nachricht oder Transaktion vermuten?

Verdächtige Nachrichten sollten per E-Mail an das Bankinstitut weitergeleitet und danach direkt gelöscht werden. Die Sparkasse beispielsweise hat dafür mit warnung@sparkasse.de eigens eine E-Mail-Adresse angelegt. Bei verdächtigen Transaktionen hingegen sollte unverzüglich der Kundenservice kontaktiert werden, um entsprechende Maßnahmen, wie zum Beispiel eine Sperrung des Online-Bankings, einzuleiten. Außerhalb der Öffnungszeiten steht den Kundinnen und Kunden hierfür die zentrale Sperrhotline 116 116 zur Verfügung.

Welche Sicherheitsregeln empfehlen Sie für das Online-Banking am Smartphone?

Im Grunde dieselben wie bei allen anderen Geräten: Es sollten nur Smartphones genutzt werden, die vom Hersteller gepflegt und regelmäßig mit Sicherheitsupdates versorgt werden. Apps sollten nur aus vertrauenswürdigen Quellen heraus installiert und auf dem aktuellen Stand gehalten werden. PINs und Passwörter sollten nicht auf dem Gerät gespeichert werden. Und selbstverständlich sollte das Smartphone mit einem sicheren, nicht leicht zu erratenden Sperrcode geschützt sein, der sehr zeitnah aktiviert wird.

Welche Risiken verbindet Ihre Bank mit dem Banking über öffentliches WLAN, und welche Empfehlungen geben Sie Ihren Kundinnen und Kunden konkret? Welche alternativen sicheren Nutzungsmöglichkeiten bewerben Sie?

Es ist grundsätzlich davon abzuraten, in einem öffentlichen WLAN sensible Daten einzugeben. Dies gilt selbstverständlich auch für das Online-Banking. Wir raten daher dazu, stattdessen die mobilen Daten (5G/4G) des eigenen Mobilfunkanbieters zu nutzen.

Welche Abläufe greifen, wenn ein Konto gehackt wurde und/oder ein Missbrauch vorliegt (zum Beispiel Sperrung, Rückbuchung, Strafanzeige)? Wie koordinieren Sie die Schnittstellen zu Ermittlungsbehörden und zur Zentralen Stelle für Betrugsbekämpfung?

Kommt es zu betrügerischen Transaktionen, werden die betroffenen Online-Banking-Zugänge unverzüglich gesperrt. Außerdem wird versucht, die betrügerischen Überweisungen mittels SEPA-Recall rückgängig zu machen. Dies gelingt allerdings nur, solange der Betrag dem Empfänger noch nicht gutgeschrieben wurde. Daher ist es zwingend erforderlich, sich sofort bei seiner Bank zu melden, sollten betrügerische Überweisungen in den Umsätzen auftauchen. Darüber hinaus sollte die oder der Geschädigte Strafanzeige bei der Polizei erstatten. Diese wendet sich dann bei Bedarf an die jeweilige Bank, um zum Beispiel Protokolle oder weitere Details anzufordern.

Welche typischen Sicherheitsfehler beobachten Sie bei Kundinnen und Kunden beim Online-Banking am häufigsten?

Der häufigste Fehler ist ganz simpel: Das Nichtlesen bzw. die Nichtbeachtung von sicherheitsrelevanten Informationen. Wir wissen beispielsweise, dass viele Kundinnen und Kunden sich die Transaktionsdetails in der pushTAN-App nicht durchlesen, sondern die Aufträge praktisch ungeprüft freigeben. Oder dass sie Aufträge am Telefon freigeben, obwohl ein expliziter Warnhinweis in der App angezeigt wird. Die entscheidenden Punkte, um sich gegen Betrug im Online-Banking zu schützen, sind daher stets, aufmerksam zu sein, Hinweise zu beachten und sich an die grundlegenden Sicherheitsregeln zu halten.

Stefanie Lettau

> Die entscheidenden Punkte, um sich gegen Betrug im Online-Banking zu schützen, sind daher stets, aufmerksam zu sein, Hinweise zu beachten und sich an die grundlegenden Sicherheitsregeln zu halten.
>
> **Sven Kietzke,**
> **Experte für das Electronic Banking**

Gerüstbau Vogel
KIEL 64 98 40
... mit uns sicher nach oben!





Maßnahmen

Wie schütze ich mich vor Schockanrufen?

Sie schützen sich vor Schockanrufen am besten, indem Sie sofort auflegen, keine persönlichen oder finanziellen Informationen preisgeben und niemals Geld oder Wertsachen an unbekannte Personen übergeben. Wenn Sie bereits auf einen Schockanruf hereingefallen sind, sollten Sie sofort die Polizei informieren und den Vorfall anzeigen.

- Vereinbaren Sie ein Familien-Kennwort, damit Sie sich gegenseitig innerhalb der Familie am Telefon identifizieren können.
- Lassen Sie sich nicht unter Druck setzen und beenden Sie das Gespräch sofort, wenn Geld gefordert wird.
- Rufen Sie Ihre Angehörigen oder Bekannten nur über eine Ihnen bekannte Nummer zurück, nicht über die Nummer aus dem Anruf.
- Nennen Sie keine Details zu Vermögen, Bankdaten, Familie oder Ihrer Wohnsituation.
- Rufen Sie die Polizei unter 110 an, wenn Ihnen der Anruf verdächtig vorkommt.
- Lassen Sie niemanden in Ihre Wohnung und übergeben Sie nichts an Fremde, auch wenn diese sich als Amtspersonen ausgeben.
- Schalten Sie Anrufer mit unbekannter Nummer auf stumm oder blockieren Sie sie. Aktivieren Sie den Spam-Schutz in den Telefon-Einstellungen.
- Reduzieren oder löschen Sie Ihren Telefonbucheintrag, damit weniger persönliche Daten öffentlich sind.
- Melden Sie sich bei Ihnen unbekannten Telefonnummern nur mit „Hallo“. Nennen Sie nicht Ihren Namen. Anrufe aus dem Ausland sollten Sie nicht annehmen, wenn Sie die Nummer nicht kennen.

Minol

Grüner Strom vom eigenen Dach mit B.One Mieterstrom.

Mit B.One Mieterstrom werden Sie zum Energieerzeuger für Ihre Mieter.

minol.de/mieterstrom

DEUTSCHES INSTITUT FÜR PRODUKT UND MARKTBEWERTUNG GMBH

ausgezeichnet für:

HOHE KUNDEN-ZUFRIEDENHEIT 2026

Basierend auf Online-Marktforschung und ausgewerteten Kundenmeinungen

www.dipmb.de/fundstelle/

Wir wollen oft glauben, was wir hoffen



Seit jeher fallen Menschen auf Betrüger herein, weshalb sich die unterschiedlichsten Ausprägungen dieses Verbrechens durch die gesamte Menschheitsgeschichte ziehen. Selbst im Tierreich gibt es Betrug. Aber warum ist das so?

Betrug ist eine Form der Manipulation. Er funktioniert nicht nur über Informationen, sondern vor allem über Emotionen. Betrüger nutzen gezielt die psychologischen Schwächen ihrer Opfer aus und brechen die sozialen Normen unseres gesellschaftlichen Miteinanders.

Wir können im Alltag nicht ständig misstrauisch sein. Häufig gehen wir daher davon aus, dass andere grundsätzlich ehrlich sind. Deshalb sind wir psychologisch auch eher darauf ausgelegt, zu kooperieren oder zu helfen. Mögliche Warnsignale werden dabei ignoriert. Haben wir in einer solchen Konstellation Kontakt mit einer Betrügerin oder einem Betrüger, die freundlich und selbstsicher auftreten, so ahnen wir daher zunächst nichts Böses. Und genau hier befindet sich das Einfallstor: Vertrauen und Hilfsbereitschaft werden ausgenutzt, ohne dass wir es zunächst vielleicht selbst bemerken.

Benutzt wird von Betrügerinnen und Betrügern auch der Wunsch nach Zugehörigkeit und Anerkennung. Jeder möchte gesehen und wahrgenommen werden. Einsamkeit und soziale Isolation steigern die Bereitschaft, einem freundlichen Kontakt zu vertrauen. Erscheint uns jemand sympathisch und glaubwürdig, neigen wir darüber hinaus dazu, widersprüchliche Hinweise nicht wahrnehmen zu wollen oder Informationen sogar so zu deuten, dass sich der erste positive Eindruck bestätigt.

Die Illusion der Kontrolle und die menschliche Gier

Wer nun von sich glaubt, schwer manipulierbar zu sein und überzeugt ist, deswegen kein Betrugsopfer zu werden, begibt sich gerade durch diese vermeintliche Selbstsicherheit in Gefahr. Die sogenannte Illusion der Kontrolle senkt die Wachsamkeit. Warnsignale werden weniger ernst genommen, da man von der eigenen Fähigkeit überzeugt ist, eine Gefahr zu erkennen.

Einer der größten Andockpunkte für Betrüger ist vielleicht die menschliche Gier. Schnelles, leicht verdientes Geld, ein hohes Gewinnversprechen oder ein einmaliges Angebot lassen so manchen den gesunden Menschenverstand vergessen. In diesem Zusammenhang arbeiten Betrügerinnen und Betrüger auch gern mit Zeitdruck. Viele Betrugsformen zielen darauf, dass Menschen schnell, intuitiv und emotional statt langsam und analytisch reagieren und handeln.

Betrüger machen bisweilen zu Beginn kleine Zusagen und erhöhen so die Wahrscheinlichkeit, dass sie ihrem Opfer im weiteren Verlauf des Kontakts größere Zugeständnisse entlocken können. Haben Menschen erst investiert, fällt es ihnen schwer, ihren Fehler einzugestehen – an bereits investiertem Geld, Zeit oder Aufwand wird oft festgehalten, obwohl ein Ausstieg sinnvoller wäre.

Im Nachhinein wird häufig versucht, das eigene Verhalten zu rechtfertigen, um so das Bild, das man von sich hat, zu schützen. Auf diese Weise kommt letztlich eine weitere Emotion ins Spiel, die von Betrügerinnen und Betrügern immer wieder ausgenutzt wird: die Scham.

Die Scham wird oft von Angst begleitet. Gemeinsam lösen diese Emotionen Stress aus und bringen die Opfer in eine Situation, in der das klare Denken beeinträchtigt ist. Betrüger erzeugen solche emotionalen Zustände ganz gezielt. So gesehen erklärt sich auch, warum selbst vorsichtige Menschen in einer akuten Betrugssituation Fehlentscheidungen treffen können.

Stefanie Lettau



Cyber-Rechtsschutz

Geschützt in der digitalen Welt

Heutzutage ist fast jeder täglich und lange im Netz unterwegs. Vorteile des Internets sind dabei Wissenszugang, Tempo, Vernetzung, Effizienz und Flexibilität. Gleichzeitig lauern Gefahren wie Datenschutzrisiken, Cyberkriminalität, soziale Risiken, Informationsflut, Fehlinformationen, Abhängigkeiten und Kommerzialisierung.

Typische Fälle und Kostenrisiko

Sie erwerben in einem Online-Shop ein Tablet für 1.800,– €, die Lieferung bleibt aus. Sie müssen die Rückzahlung des Geldes auf dem Klageweg mit einem Kostenrisiko von 1.500,– € durchsetzen.

Im sozialen Netzwerk haben Sie ein Foto hochgeladen und erhalten eine Abmahnung wegen eines angeblichen Urheberrechtsverstoßes, da Sie keine Genehmigung dafür hatten. Hierfür übernimmt die ÖRAG die Anwaltskosten bis zu 1.000,– €.

Ihr Kind ist in Sozialen Netzwerken unterwegs und wird dort von einer Person gemobbt, indem diese unwahre Behauptungen über Ihr Kind verbreitet (Cybermobbing). Sie möchten eine Strafanzeige bei der Polizei fertigen. Hierfür übernimmt die ÖRAG die Anwaltskosten (Kostenrisiko 500,– €).

Absicherung

Daher deckt der Privat-Rechtsschutz unseres Kooperationspartners ÖRAG Rechtsrisiken des Alltags ab und umfasst auch den Cyber-Rechtsschutz:
https://www.hausundgrund.de/verband/schleswig-holstein/oerag

Für die Rechtsfragen rund um Ihre Immobilie steht Ihnen selbstverständlich weiterhin Ihr Haus & Grund-Ortsverein zur Seite sowie die ergänzenden Versicherungen der ÖRAG.

Was passiert mit den Opfern, wenn die Polizei gegangen ist?



WWW.POLIZEI-BERATUNG.DE

Diese Frage hat sich der ehemalige Fernsehmoderator Eduard Zimmermann (Aktenzeichen XY) gestellt und 1976 die Gründung des WEISSEN RINGS initiiert.

In Schleswig-Holstein befindet sich das Landesbüro des Vereins in Rendsburg. Zwei festangestellte Mitarbeiterinnen arbeiten hier in der Verwaltung. Alles weitere wie unter anderem die Präventionsarbeit und die Opferberatung werden ehrenamtlich geleistet.

Stefan Klein und Erik Grünberg sind zwei dieser ehrenamtlichen Mitarbeiter in Schleswig-Holstein. Beide sind in der Opferberatung tätig, Klein ist zudem Präventionsbeauftragter.

„Nach einer Straftat steht der WEISSE RING einem Opfer zunächst einmal in seiner Lotsenfunktion zur Verfügung. Wir hören zu und versuchen ein gewisses Maß an Stabilität und Struktur zurückzugeben. Der Gedanke dahinter ist: Hilfe zur Selbsthilfe“, erklärt Erik Grünberg. Es sei entscheidend, den Betroffenen frühzeitig wieder das Gefühl zu geben, dass sie selbst über alle Dinge bestimmen, die sie tun. Insbesondere nach Gewalt oder Gewaltstraftaten würden Leidtragende häufig einen Kontrollverlust erleiden. „Da müssen wir mit viel Fingerspitzengefühl versuchen, einfach nur eine Stütze zu sein und den Menschen helfen, die Kontrolle über ihr Leben zurückzugewinnen.“

In dem Deliktsfeld rund um Betrug ist dagegen Scham das eigentliche Kernthema. „Der finanzielle Verlust ist natürlich auch belastend, aber im Mittelpunkt steht für die Betrogenen viel mehr der innere Vorwurf und die quälende Frage, wie sie darauf hereinfallen konnten. Nicht selten hören sie diesen Vorwurf auch aus dem engsten sozialen Umfeld, von Familie und Freunden“, sagt Grünberg dazu. „Und genau das muss man einfangen und den Menschen vermitteln, dass sie nicht allein sind mit diesem Thema. Es kann jeden treffen. Die Täterstrukturen, mit denen wir heute zu tun haben, sind hochprofessionell. Und ich versuche den Opfern auch immer mitzugeben, dass die Scham nicht ihnen, sondern dem Täter gehört.“

Ist der Verlust sehr groß, und sind durch das eigene Verhalten auch andere wie die eigene Familie betroffen, können die Folgen zerstörerisch sein. „Gerade im Zusammenhang mit Schockanrufen und dem sogenannten Enkeltrick sind auch Suizide von Betroffenen bekannt geworden“, weiß Grünberg. „Da war die Scham so groß, dass die Menschen keinen anderen Ausweg mehr gesehen haben.“ Deshalb versuchen die Mitarbeiter des WEISSEN RINGS in solchen Fällen zusätzlich auf das soziale Umfeld des Opfers einzuwirken, damit die Betrogenen sich nicht auch noch dessen Vorwürfen ausgesetzt sehen.

Die Arbeit an einem Fall beginnt für Grünberg in der Regel mit einem Anruf seitens eines Opfers einer Tat beim Leiter einer Außenstelle. Es folgt ein Erstgespräch mit ihm als Opferberater, bei dem auch ein Termin für ein Treffen verabredet wird, das in der Regel an einem neutralen Ort stattfindet. „Im ersten Gespräch hört man den Betroffenen einfach nur zu. So bekomme ich auch ein Bild, wie er oder sie mit ihrer Opferrolle umgehen. Das ist nämlich sehr unterschiedlich. Einige werden richtig aktiv, die gehen sozusagen in den Widerstand, andere sind wie paralysiert.“

> Ich versuche, den Opfern immer mitzugeben, dass die Scham nicht ihnen, sondern dem Täter gehört.
>
> **Erik Grünberg, Ehrenamtlicher Mitarbeiter WEISSER RING**

Die Opferberater vermitteln auch Kontakte in Trauma-Ambulanzen, zu Anwälten und in Selbsthilfegruppen. Sie helfen den Betroffenen beim Erstellen von Strafanzeigen, begleiten sie zu Gerichtsterminen und bei Zeugenaussagen. „Viele haben so etwas noch nie gemacht und es hilft ihnen ungemein, wenn wir die ganzen Verfahren transparent machen, indem wir erzählen, was sie erwartet“, so Grünberg.

Die künftigen Opferberater erhalten für ihre Tätigkeit im Rahmen von Schulungen eine Qualifikation, die mit einer Hospitation beginnt, während derer sie schon aktive Berater begleiten, um auf diese Weise festzustellen, ob sie sich für die ehrenamtliche Arbeit in diesem Segment überhaupt eignen.

„Es ist nicht einfach, beispielsweise ein Gespräch mit der Mutter einer oder eines Getöteten zu führen“, sagt Stefan Klein dazu. Der WEISSE RING unterhält eine eigene Akademie, die extra für die Schulungen und Fort- und Weiterbildung zum Opferberater da ist. „Da treten nicht nur Mitarbeiter des WEISSEN RINGS auf, sondern auch Psychologen und Therapeuten und durchaus auch ein Mitarbeiter des Bundeskriminalamts“, erklärt Klein. „Wir brauchen diese Fachleute, die von außen kommen und uns aus dem Berufsleben heraus schulen, sodass wir auf dem Stand der Dinge bleiben.“

Die Beratung macht natürlich auch etwas mit den Beratenden. Der Umgang mit Menschen in Not und Verzweiflung, die Konfrontation mit Gewalt und Verbrechen. Wie wird das aufgearbeitet? „Wir machen eine sogenannte kollegiale Fallbearbeitung“, erklärt Klein. „Und in Mainz, unserer zentralen Geschäftsstelle, haben wir jemanden, der Supervision macht und gegebenenfalls auch in die Außenstellen kommt.“

Aber nicht nur die Opferberatungen sind ein wichtiger Teil der Arbeit des WEISSEN RINGS. Ganz vorne steht die Prävention. Damit Menschen erst gar nicht zu Opfern von Verbrechen werden. Stefan Klein besucht Vereine und Verbände, Landfrauen und Seniorenvereinigungen und klärt unter anderem auf über Betrugsdelikte im Internet oder Schockanrufe. In Schleswig-Holstein gibt es 16 Außenstellen, an die Interessierte sich wenden können, um eine solche Aufklärung in ihrem eigenen Verein anzubieten.

„Ich habe vor einiger Zeit eine E-Mail von einer Frau erhalten, die an einer meiner Veranstaltungen teilgenommen hat und sich ausdrücklich bedankt hat, weil unsere Ratschläge direkt geholfen haben“, erzählt Klein. „Die 96-jährige Mutter der Frau hatte einen Schockanruf bekommen, angeblich sei ihre Tochter in Not. Geistergegenwärtig hat die alte Dame nach dem Familienpasswort gefragt. Da hat der Anrufer sofort aufgelegt.“

Stefan Klein und Erik Grünberg verbringen viel Zeit im Rahmen ihres Ehrenamtes – mit den Menschen, denen sie helfen, aber auch bei regelmäßigen Fort- und Weiterbildungen, die oft an Wochenenden stattfinden. Was gibt ihnen diese Tätigkeit? „Ich erlebe direkt die Wirksamkeit meines Handelns im Austausch mit den Betroffenen“, sagt Grünberg dazu. „Außerdem habe ich auf diese Weise die Möglichkeit, der Gesellschaft etwas zurückzugeben mit einer Hilfe, die an der richtigen Stelle wirkt. Denn hier gibt es eine Lücke, die einfach institutionell da ist. Im Strafprozess geht es primär immer um den Täter. Ganz oft bleiben die Opfer und auch ihre Familien zurück. Es ist eine äußerst sinnstiftende Tätigkeit, hier helfen zu können. Das gibt mir ein wirklich gutes Gefühl.“

Wer sich für eine Präventionsveranstaltung interessiert, kann sich an die für ihn zuständige Außenstelle des WEISSEN RINGS in Schleswig-Holstein wenden.

› https://schleswig-holstein.weisser-ring.de/

Stefanie Lettau



Stefan Klein



Erik Grünberg



Organisation

683.859

Menschen wurden betreut, die Opfer von Gewalt geworden sind.

In 50 Jahren WEISSER RING (Stand April 2026)

Mit einem Netz aus 18 Landesverbänden und 400 Außenstellen ist der WEISSE RING bundesweit die größte Hilfsorganisation für Opfer von Kriminalität. 40.000 Mitglieder unterstützen den Verein, der sich über monatliche Mitgliedsbeiträge, Spenden, Nachlässe und Geldbußen, die von Gerichten und Staatsanwaltschaften verhängt werden, finanziert. Rund 3.000 Helferinnen und Helfer engagieren sich in ganz Deutschland ehrenamtlich für die Opfer von Straftaten.

Der Verein leistet seine Hilfe unabhängig von einer Mitgliedschaft. Zu den Hilfsmaßnahmen gehören unter anderem

- menschlicher Beistand und persönliche Betreuung nach einer Straftat
- Begleitung zu Terminen bei Polizei, Staatsanwaltschaft und Gericht
- Hilfeschecks für eine anwaltliche Erstberatung sowie für eine rechtsmedizinische Untersuchung
- Übernahme von Anwaltskosten, insbesondere zur Wahrung von Opferschutzrechten im Strafverfahren und zur Durchsetzung von Ansprüchen nach dem Opferentschädigungsgesetz
- Erholungsmaßnahmen in bestimmten Fällen
- finanzielle Unterstützung zur Überbrückung tatbedingter Notlagen
- Vermittlung von Hilfen anderer Organisationen

Neben der aktiven Opferhilfe fordert der Verein von Politik, Justiz und Verwaltung die Verbesserung der rechtlichen und sozialen Situation von Kriminalitätsopfern und ihren Angehörigen. Der WEISSE RING kämpft außerdem für ein stärkeres gesellschaftliches Bewusstsein für die Situation der Opfer. *Stefanie Lettau*

Opfer-Telefon:
116 006, bundesweit,
kostenfrei, täglich 7.00 bis 22.00 Uhr
Online-Beratung:
www.weisser-ring.de/hilfe-fuer-opfer/onlineberatung
Spendenkonto:
IBAN: DE26 5507 0040 0034 3434 00,
BIC: DEUTDE5MXXX, Deutsche Bank Mainz



Tipps

Mehr Sicherheit im Internet

Zu den derzeit häufigsten Betrugsmethoden im Internet gehören **Phishing, Fake-Shops, Abo-Fallen, Love-Scamming, Anlagebetrug, Fake-Kundenservice, CEO-Fraud und Gewinnspiel-/Lotterie-Betrug.** Wenn Sie darauf stoßen, sollten Sie nicht reagieren, nichts bezahlen, keine Daten preisgeben und den Vorfall sofort sichern und melden.

- Öffnen Sie keine unbekannten Anhänge in E-Mails, SMS oder Textnachrichten. Gehen sie im Zweifelsfall über die offizielle Website des Absenders, sofern er Ihnen bekannt ist. Geben Sie keine persönlichen Daten, Passwörter oder Bankdaten am Telefon oder im Internet an unbekannte Personen weiter. Geben Sie Daten nur auf vertrauenswürdigen Websites ein und achten Sie darauf, dass die Verbindung verschlüsselt ist (https).

- Starten Sie Downloads nur aus seriösen Quellen, am besten direkt von der Hersteller- oder Anbieterwebsite.

- Installieren Sie regelmäßig Updates für Betriebssystem, Apps und Programme, damit bekannte Sicherheitslücken geschlossen werden.

- Nutzen Sie das öffentliche WLAN nicht für Online-Banking oder Einkäufe im Internet.

- Leisten Sie bei Online-Shops keine Vorkasse ohne Prüfung. Es gibt inzwischen auch Fake-Shop-Finder bei bestimmten Landeskriminalämtern.

- Vertrauen Sie keinen Investitionsangeboten aus Social Media oder Social-Media-Messengern. Auch sehr professionelle Webauftritte können heutzutage mit Hilfe von KI nur vorgetäuscht sein.

- Schicken Sie keine intimen Fotos oder Videos an Online-Kontakte, die Sie vorher nie persönlich getroffen haben. Selbst wenn Sie vermeintlich schon eine gute Vertrauensbeziehung aufgebaut haben, bleiben Sie skeptisch.

- Geben Sie auf Social Media nichts von sich preis, was über den eigenen Namen hinausgeht. Es gibt Kriminelle, die Social-Media-Profile gezielt verfolgen, um beispielsweise zu erfahren, wann die Betroffenen im Urlaub sind, um so einen Einbruch zu planen.

- Nutzen Sie KI, um Websites, Anbieter und Firmen auf ihre Glaubwürdigkeit zu überprüfen.

- Beachten Sie die Persönlichkeitsrechte Ihrer Kinder und Enkel. Stellen Sie keine Fotos von Minderjährigen bei Social Media oder ins Internet ein.





EigenVerwaltungPLUS

Sie möchten Ihre Immobilien digital verwalten? Kein Problem, denn mit unserer Software EigenVerwaltungPLUS können Sie alles digital und selbstständig erledigen – ohne lästigen Papierkram und Excel-Tabellen.

Haus & Grund®
Eigentum. Schutz. Gemeinschaft.
Verlag & Service GmbH Kiel



Mediaberatung
Merle Schneider
Tel. 0151 11 07 58 61

Stoppen. Hinterfragen. Schützen.

Jeder kann Opfer eines Internetbetrugs werden, ob Anwalt, Ärztin, Student oder Rentnerin

Der Zugang zu Internet und Social Media macht für viele Menschen in vielerlei Hinsicht das Leben leichter. Alltägliche Informationen und allgemeingültiges Wissen sind für jeden mit wenigen Clicks verfügbar, und die Kommunikation mit Familie und Freunden wird erleichtert, selbst wenn große Entfernungen zu überbrücken sind. Die soziale Teilhabe hat aber auch ihren Preis. Denn es lauern Gefahren. Jeder hat schon einmal die entsprechenden Begriffe gehört, ob es um das sogenannte Love Scamming geht, um Schockanrufe oder Online-Betrug zum Beispiel bei Kauf- oder Investitionsangeboten, bei Lotterie- und Glücksspielangeboten oder beim Buchen von Ferienwohnungen.



Stoppen.Hinterfragen.Schützen lautet die zentrale Präventionsbotschaft der Polizei, um nicht Opfer eines Betrugs zu werden.

Die Täter passen ihre Methoden laufend an und kombinieren zunehmend Telefon, Messenger, soziale Netzwerke, gefälschte Internetseiten und weitere digitale Kommunikationswege. Auch Künstliche Intelligenz kann mittlerweile eingesetzt werden, etwa zur Erzeugung gefälschter Stimmen oder Bilder.

Das Landeskriminalamt Schleswig-Holstein (LKA SH) stellt dazu fest, dass bei den genannten Delikten eine zunehmende Professionalisierung und Arbeitsteilung stattfindet. Gerade beim Callcenter-Betrug stehen häufig organisierte und international agierende Tätergruppen hinter den Taten, die unter anderem in der Türkei und Osteuropa professionelle Callcenter-Strukturen unterhalten. Dabei können unterschiedliche Personen unterschiedliche Aufgaben übernehmen: vom Erstkontakt über die Gesprächsführung bis hin zur Organisation von Geld- oder Wertgegenstände-Abholungen oder Weiterleitung erbeuteter Vermögenswerte.

Die Täter agieren oftmals überregional und grenzüberschreitend und nutzen technische sowie organisatorische Maßnahmen zur Verschleierung ihrer Identität und ihres Aufenthaltsortes. Diese arbeitsteilige Vorgehensweise erschwert die Identifizierung einzelner Tatbeteiligter und stellt besondere Anforderungen an die Ermittlungsbehörden. Allerdings sollte nicht davon ausgegangen werden, dass hinter jedem Betrugsfall eine große Organisation steht. Das Spektrum reicht tatsächlich von Einzeltätern über arbeitsteilige Gruppen bis hin zu hochprofessionellen, international agierenden kriminellen Netzwerken.

Beim Enkeltrick, Schockanruf und anderen Formen des Callcenter-Betrugs sind insbesondere ältere Menschen eine wichtige Zielgruppe. Die Täter wählen diese Opfer teilweise gezielt aus, zum Beispiel über ihren Telefonbucheintrag, und versuchen, deren Hilfsbereitschaft gegenüber Angehörigen beziehungsweise das Vertrauen in staatliche Institutionen auszunutzen. Die Täter arbeiten mit professionellen psychologischen Manipulationstechniken und erzeugen bewusst eine Ausnahmesituation, sagt das LKA SH dazu.

Beim Online-Betrug ist die Situation anders: Grundsätzlich kann hier jeder zum Opfer werden unabhängig von Bildungsstand, Alter oder Geschlecht. Die konkrete Betrugsmasche wird häufig auf die Lebenssituation und Interessen des potenziellen Opfers zugeschnitten.

Beim Love Scamming wiederum, was überwiegend aus dem Ausland begangen wird, können beispielsweise Menschen angesprochen werden, die auf Dating-Plattformen oder sozialen Netzwerken nach einem Partner suchen. Die Täter versuchen, emotionale Nähe und Vertrauen aufzubauen und nutzen diese Beziehung anschließend finanziell aus. Hier ist das wichtigste Warnsignal häufig nicht eine einzelne Nachricht, sondern die Entwicklung der Beziehung hin zu einer sehr schnellen emotionalen Nähe mit Liebesbekundungen und einer gemeinsamen Zukunftsplanung, ohne dass jedoch ein tatsächliches persönliches Treffen stattfindet. Irgendwann folgen eine angebliche Notlage und die Bitte um Geld, Gutscheine oder Kryptowährungen.

Besonders aufmerksam sollte man grundsätzlich dann werden, so das LKA SH, wenn die Person, mit der man Kontakt hat, ungewöhnlich großen Zeitdruck erzeugt, eine Situation ausdrücklich geheim gehalten werden soll, Geld oder sensible Daten verlangt werden, eine Zahlung ausschließlich über ungewöhnliche Wege erfolgen soll, Zugangsdaten, PINs oder TANs abgefragt werden oder die Kommunikation mit einer vermeintlich bekannten Person plötzlich befremdlich wirkt.

Die zentrale Präventionsbotschaft lautet: **Stoppen – Hinterfragen – Schützen.** Was nichts anderes heißt als: Nicht sofort reagieren, sondern einen Schritt zurücktreten und die Situation in Ruhe und gegebenenfalls über einen unabhängigen Kommunikationsweg überprüfen.

Zeit bedeutet Ermittlungserfolg

Wer in welcher der genannten Formen auch immer Opfer eines Betrugs geworden ist, sollte auf jeden Fall eine Anzeige bei der Polizei stellen, auch wenn der Betrugsversuch erfolglos geblieben ist. Denn eine Anzeige dient nicht nur dazu, einen individuellen Schaden zu verfolgen. Sie ist gleichzeitig ein wichtiger Beitrag zur Erkennung des tatsächlichen Kriminalitätsgeschehens. Die Polizeiliche Kriminalstatistik kann nur das sogenannte Hellfeld abbilden – also Straftaten, von denen die Polizei Kenntnis erhält.

Gerade bei Betrugsdelikten ist jedoch das Dunkelfeld groß. Das BKA hat für 2024 beispielsweise festgestellt, dass bei Betrugsfällen, bei denen sich Täter als jemand anderes ausgeben – etwa beim Enkeltrick –, die Anzeigequote lediglich bei rund 40 Prozent lag. Das bedeutet zugleich: Ein erheblicher Teil dieser Taten wird der Polizei nicht bekannt und kann somit nicht in die statistische Ermittlung einfließen, die wiederum auch Einfluss nimmt auf die politische Betrachtung einzelner Kriminalitätsfelder und die Besetzung von Dienstposten.

Eine Anzeige kann zudem dazu beitragen, Täterstrukturen zu erkennen, gleiche Tatmuster miteinander zu verknüpfen, Ermittlungsansätze zu gewinnen und Präventionsmaßnahmen zielgerichteter auszurichten. Entscheidend ist dabei auch, die Anzeige möglichst zeitnah zum Vorfall zu stellen. Bei Betrugsdelikten können Accounts gelöscht, Anzeigen entfernt, Telefonnummern gewechselt, E-Mail-Adressen aufgegeben oder Webseiten abgeschaltet werden. Auch Zahlungswege sind in der Regel nur für einen begrenzten Zeitraum nachvollziehbar.

Stefanie Lettau

Wir wollen, dass Sie sicher leben. Ihre Polizei

Entscheidend ist weniger die Frage, ob jemand ‚vorsichtig genug' ist. Entscheidend ist, ob Menschen die typischen Manipulationsmuster erkennen und in einer überraschenden Situation innehalten können.

Landeskriminalamt S.-H.

Haus & Grund®
Eigentum. Schutz. Gemeinschaft.
Immobilien GmbH Kiel

Michaela, Thomas und Helena Hanzlik,
Haus & Grund-Mitglied seit 2005





WWW.POLIZEI-BERATUNG.DE

Der Trick an der Haustür

Beliebt bei Kriminellen sind Tricks an der Haustür. Das Ziel ist dabei immer, in die Wohnung zu gelangen, um Bargeld, Schmuck oder andere Wertsachen zu entwenden. Dabei sind die Täterinnen und Täter sehr kreativ. Sie bedienen sich unter anderem folgender Maschen: Sie bitten beispielsweise um Hilfe oder eine Gefälligkeit, fragen nach einem Glas Wasser oder nach etwas zum Schreiben. Andere möchten die Toilette oder das Telefon benutzen oder Geschenke für Nachbarn abgeben.

Es gibt auch solche, die sich als Amtsperson ausgeben und behaupten, die Wohnung betreten zu müssen, zum Beispiel als Polizistin, Polizist oder Gerichtsvollzugsperson. Wiederum andere geben sich als Mitarbeitende beispielsweise von Elektrizitätswerken aus oder behaupten, von der Hausverwaltung, der Kirche, von Versicherungen, Telefongesellschaften oder Umfrageinstituten zu kommen. Sie täuschen technische Notfälle (Gasleck, Wasserschaden oder ähnliches) vor, um mit dieser vermeintlichen Gefahrensituation künstlich Druck zu erzeugen.

Ein weiterer Trick besteht darin, vorzutäuschen, die Wohnungsinhaberin oder den -inhaber zu kennen, zum Beispiel aus der entfernten Verwandtschaft zu kommen, früher in der Nachbarschaft gewohnt zu haben oder als Kollegin oder Kollege zusammengearbeitet zu haben.

Bei Handwerkern und Servicemitarbeitern sollte man sich fragen: Habe ich diese Person oder dieses Unternehmen überhaupt bestellt? Wurde der Besuch von meiner Hausverwaltung angekündigt? Kann ich die Firma selbst über eine bekannte Telefonnummer erreichen? Gibt es einen nachvollziehbaren Auftrag? Und: Wird Druck aufgebaut, sofort handeln oder bezahlen zu müssen?

Bei angeblichen Amtspersonen sollte der Dienstausweis verlangt werden. Im Zweifel sollte die betreffende Behörde selbst kontaktiert werden. Wichtig ist dabei, die Telefonnummer nicht einfach von der unbekannten Person zu übernehmen, sondern sie selbst herauszusuchen. Im Zweifel sollte man den polizeilichen Notruf 110 wählen, um zu überprüfen, ob es sich um echte Polizeibeamte handelt.

Als besonders wichtiges Warnsignal gilt, wenn die Person versucht, eine Überprüfung zu verhindern oder behauptet, dass die Situation eine sofortige Entscheidung erfordert.

Grundsätzlich sollte man keine persönlichen oder finanziellen Informationen an unbekannte Personen herausgegeben. Das gilt auch für Bargeld und Wertgegenstände.

Weitere Information gibt es unter **www.polizei-beratung.de** und **www.polizei-beratung.de/themen-und-tipps/sicher-handeln/die-shs-regel/**

Stefanie Lettau

> Wenn sich eine Situation verdächtig anfühlt, sollte zunächst die eigene Sicherheit im Vordergrund stehen. Man sollte nicht selbst eine riskante Konfrontation suchen, sondern die Polizei unter 110 rufen.
>
> **Landeskriminalamt S.-H.**

Doppelt hält besser

E-Paper gratis im Print-Abo



Einmal aktiviert, überall informiert

Ab sofort lesen Sie Ihre Zeitung, wann und wo Sie möchten.

www.kn-online.de/aktivieren

Kieler Nachrichten

Partner im RedaktionsNetzwerk Deutschland

techem

Sicher vermieten. Weniger Aufwand.

Digitale, einfache und rechtskonforme Lösungen für Ihre Immobilie.



Egal, ob Sie 2 oder 20 Wohneinheiten vermieten, mit Techem haben Sie den richtigen Partner. Wir unterstützen Sie mit unseren Lösungen von Heizkostenabrechnung über Rauchwarnmelder bis zur Legionellenprüfung. Rechtskonform, einfach, verlässlich.
Gerne beraten wir Sie persönlich unter **06196 522-7970** (Mo–Fr 8–17 Uhr), oder senden Sie eine E-Mail an **privatkundenvertrieb@techem.de**. Mehr Infos finden Sie unter **techem.de/loesungen**