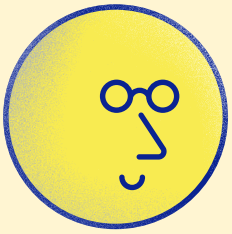
Wie man Scamming erkennt und vermeidet



Ihr Leitfaden zum Schutz vor Scamming (Internet- und Telefonbetrug)

Australian Government

National Anti-Scam Centre

ScamWatch
Stop. Better safe than scammed.

Anerkennung des indigenen Landes

Die ACCC würdigt die traditionellen Eigentümer und Hüter des indigenen Landes in ganz Australien sowie ihre fortdauernde Verbindung zu Land, Wasser und Gemeinschaften. Wir zollen ihnen und ihren Kulturen sowie ihren Ältesten der Vergangenheit, Gegenwart und Zukunft unseren Respekt.

Australian Competition and Consumer Commission
Ngunnawal
23 Marcus Clarke Street, Canberra, Australian Capital Territory, 2601

ACCC 05/24_24-13

www.accc.gov.au

Inhalt

Dieser Leitfaden wurde vom National Anti-Scam Centre verfasst und soll Ihnen helfen, Scamming zu erkennen und sich davor zu schützen.

Scamming ist ein Verbrechen, und Menschen, die Scamming begehen, sind Kriminelle. Viele Menschen in Australien werden Opfer von Scamming und verlieren ihr Geld, manchmal sogar ihre gesamten Ersparnisse. Scamming schadet dem Leben der Menschen.

Scamming ist immer schwieriger zu erkennen, deshalb müssen wir es zusammen stoppen.

Das National Anti-Scam Centre setzt sich für den Schutz aller Australierinnen und Australier vor Scamming ein.

Wir suchen in Zusammenarbeit mit der Regierung und der Wirtschaft neue Wege, um Scammer daran zu hindern, Geld und persönliche Daten von Australiern zu stehlen. Hier sind einige der Wege, über die wir dies erreichen.

Wir helfen Menschen, Scamming zu erkennen und zu vermeiden

Über Scamwatch informieren wir über aktuelle Scamming-Maschen und Möglichkeiten, wie Sie sich vor Scamming schützen können.

Wir machen Scammern das Leben schwer

Indem wir Informationen sammeln und zwischen staatlichen Stellen und der Wirtschaft austauschen, machen wir es Scammern schwerer, weiterhin Straftaten zu begehen, und erleichtern es der Bevölkerung, Scamming zu melden.

Hilfe ist verfügbar

Wenn Sie dies lesen, sind Sie oder jemand, den Sie kennen, wahrscheinlich schon einmal Opfer von Scamming geworden. Leider sind Sie nicht allein. Scamming wird immer raffinierter, sodass jeder zum Opfer werden kann.

Wenn Sie Opfer von Scamming geworden sind, ist es wichtig, dass Sie schnell handeln.

Wenn Sie Geld an einen Scammer verloren haben, wenden Sie sich an Ihre Bank oder Ihren Kartenanbieter.

Wenden Sie sich an IDCARE, 1800 595 160, www.idcare.org

Scamming ist oft erfolgreich, weil ein realistischer Eindruck vermittelt wird. Scammer verlassen sich darauf, dass Sie Warnzeichen übersehen, weil Sie es eilig haben, weil etwas nach einem tollen Angebot aussieht, das Sie sich nicht entgehen lassen wollen, oder weil es von jemandem zu kommen scheint, dem Sie vertrauen.

Schützen Sie sich vor Scamming, indem Sie diese 3 Schritte befolgen:

Halt

Geben Sie niemandem Geld oder persönliche Daten, wenn Sie sich nicht sicher sind.

Scammer bieten Ihnen oft Hilfe an oder bitten Sie, Ihre Identität zu bestätigen. Sie geben sich als Vertreter von Organisationen aus, die Sie kennen und denen Sie vertrauen, z. B. von Dienstleistern, der Polizei, Ihrer Bank oder staatlichen Stellen.

Prüfen

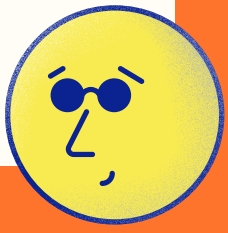
Fragen Sie sich – könnte eine Nachricht oder ein Anruf gefälscht sein?

Klicken Sie niemals auf einen Link in einer Nachricht. Kontaktieren Sie Unternehmen oder staatliche Stellen nur über Kontaktdaten, die Sie selbst auf den jeweiligen offiziellen Websites oder in der offiziellen App finden. Wenn Sie sich nicht sicher sind, sagen Sie „Nein“ und legen Sie auf bzw. löschen Sie die Nachricht.

Melden

Handeln Sie schnell, wenn sich etwas nicht richtig anfühlt.

Wenden Sie sich an Ihre Bank, wenn Sie ungewöhnliche Aktivitäten bemerken oder wenn ein Scammer Ihr Geld oder Ihre Daten erhalten hat. Suchen Sie Hilfe und melden Sie Scamming bei ReportCyber und Scamwatch. Wenn Sie Scamming melden, helfen Sie allen Australiern, denn so stärken Sie unsere Abwehr.



Was ist Scamming?

Scamming liegt vor, wenn jemand Sie täuscht, um Ihr Geld oder Ihre persönlichen Daten zu stehlen.

Scamming ist ein Wirtschaftsverbrechen, das von Kriminellen begangen wird, die oft sehr raffiniert und gut organisiert sind.

Scamming:

- ✓ wird von Kriminellen begangen
- ✓ erscheint echt
- ✓ wird von glaubwürdigen Geschichten begleitet
- ✓ setzt Sie unter Druck, bestimmte Dinge zu tun

Folgendes ist KEIN Scamming:

- ✗ Computer - Hacking
- ✗ Missbräuchliche Vertragsklauseln
- ✗ Belästigende Marketing-Ansätze

Es ist wichtig zu wissen, dass nicht alle negativen Erfahrungen Scamming darstellen. Vielleicht haben Sie für ein Produkt bezahlt, das Sie nie erhalten haben, oder Sie haben etwas gekauft und festgestellt, dass die Qualität mangelhaft war. Dies ist zwar enttäuschend, aber es handelt sich nicht unbedingt um Scamming. Das australische Verbrauchergesetz bietet australischen Verbrauchern Schutz bei dieser Art von Problemen.

Weitere Informationen erhalten Sie unter www.accc.gov.au/consumers.

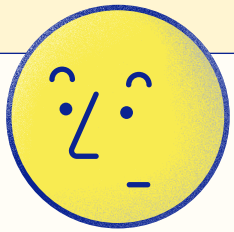
Einfache Schritte zur Erkennung und Vermeidung von Scamming

Wir alle können von Scamming betroffen werden. Scamming funktioniert, weil Scammer glaubwürdige Geschichten erfinden, um Ihr Geld zu stehlen und Ihre persönlichen Daten zu erhalten.

Scammer werden zunehmend cleverer und nutzen neue Technologien, Produkte, Dienstleistungen und wichtige Ereignisse, um Sie davon zu überzeugen, dass ihre Betrügereien echt sind.

Es kann sehr schwer sein, Scamming zu erkennen. Hier sind einige Situationen, bei denen Sie vorsichtig sein sollten. Manchmal verwenden Scammer eine Kombination dieser Taktiken.

1. **Möglichkeiten, Geld zu verdienen oder zu sparen:** Scammer gaukeln Ihnen vor, dass Sie ein einzigartiges Angebot erhalten. Sie setzen Sie unter Druck, schnell zu handeln, damit Sie die Gelegenheit nicht verpassen. Denken Sie daran: Angebote, die zu schön sind, um wahr zu sein, haben im Allgemeinen einen Haken.
2. **Traurige Geschichten und Bitten um Hilfe:** Scammer versuchen, Ihre Gutmütigkeit auszunutzen. Sie erzählen Ihnen Geschichten von Herzschmerz und Tragödien und erklären, warum sie Ihre Hilfe und Ihr Geld brauchen.
3. **Links und Anhänge:** Scammer verwenden Links, um Sie zu betrügerischen Websites zu leiten, die darauf abzielen, Ihre Daten und Ihr Geld zu stehlen. Möglicherweise werden Sie auch aufgefordert, Anhänge zu öffnen. Diese können Viren installieren, die Ihre Daten stehlen.



4. **Druck, schnell zu handeln:** Scammer wollen nicht, dass Sie sich Zeit nehmen und die Dinge überdenken. Sie wollen Sie unter Druck setzen, damit Sie schnell handeln. Dies kann selbst Drohungen beinhalten, dass etwas Schlimmes passiert, wenn Sie nicht sofort handeln.
5. **Aufforderungen, auf ungewöhnliche oder spezielle Weise zu zahlen:** Scammer fordern Sie oft auf, mit ungewöhnlichen Methoden wie mit vorab aufgeladenen Debitkarten, iTunes-Karten oder virtuellen Währungen wie Bitcoin zu bezahlen. Ist dieses Geld einmal ausgegeben, können Sie es nicht mehr zurückbekommen.
6. **Aufforderung zur Einrichtung neuer Konten oder PayIDs:** Scammer können Sie auffordern, ein neues Bankkonto oder eine PayID einzurichten, um sie zu bezahlen (oder von ihnen bezahlt zu werden). Sie geben sich möglicherweise als Ihre Bank aus und fordern Sie auf, Ihr Geld auf neue Konten zu überweisen, damit es sicher ist.

Wenn Scammer einmal erfolgreich Geld von Ihnen erbeutet haben, versuchen sie, noch mehr Geld von Ihnen zu bekommen. Leider wird eines von drei Scamming-Opfern mehr als einmal betrogen. Wenn Sie durch Scamming Geld verloren haben, seien Sie besonders vorsichtig, da Scammer Ihnen eventuell ihre Hilfe anbieten, damit Sie Ihr Geld zurückbekommen. Dies ist eine Art von Folgebetrug.

Textnachricht-/SMS-Scamming

Scammer senden Nachrichten, die vorgeblich von staatlichen Stellen, Strafverfolgungsbehörden, vertrauten Unternehmen oder gar Mitgliedern Ihrer Familie oder Freunden kommen.

Diese Nachrichten klingen dringend und versuchen, Sie zum schnellen Handeln zu bewegen. Sie enthalten oft einen Link, der Sie zu einer betrügerischen Website leitet. Scammer können alle persönliche Daten, die Sie auf diesen betrügerischen Websites eingeben, stehlen und dazu verwenden, Ihr Geld zu erbeuten oder in Ihrem Namen einen Betrug zu begehen.

Um diese Nachrichten echt erscheinen zu lassen, kopieren oder verschleiern Scammer ihre Telefonnummer hinter der Telefonnummer und der Anrufer-ID von seriösen Unternehmen oder Menschen, die Sie kennen.

Scamming-Nachrichten können sogar im gleichen Nachrichtenverlauf wie echte Nachrichten eines Unternehmens erscheinen, was ihre Erkennung noch schwieriger macht.

Anzeichen, dass eine Nachricht Scamming sein könnte

Die Nachricht:

Fordert Sie auf, sofort zu handeln, eine Zahlung zu leisten oder Geld zu überweisen

Fordert Sie auf, auf einen Link zu klicken oder eine in der Nachricht angegebene Nummer anzurufen

Fordert Sie auf, sich mit Ihrem Benutzernamen und Passwort bei einem Online-Konto anzumelden oder andere persönliche Daten anzugeben

Stammt von einem Familienmitglied oder Bekannten, das/der mitteilt, dass sich seine Kontaktdaten geändert haben

Droht an, eine Dienstleistung einzustellen oder Ihnen Gebühren in Rechnung zu stellen, wenn Sie nicht handeln

Suggeriert, dass Sie oder Ihre Konten gehackt wurden oder in Betrug verwickelt sind

Suggeriert, dass es ein Problem mit Ihrer Zahlung oder der Zustellung Ihres Pakets gibt

Schritte, um sich vor Scamming-Nachrichten zu schützen

1. Wenn jemand, den Sie kennen, Ihnen eine Nachricht schickt, dass er eine neue Telefonnummer hat:
   - **a.** versuchen Sie, diese Person unter der bestehenden Nummer anzurufen, die Sie für sie haben, und
   - **b.** senden Sie dieser Person unter der neuen Nummer eine Nachricht mit einer Frage, auf die nur sie die Antwort kennt, um die Identität der Person zu prüfen.

2. Klicken Sie niemals auf Links in Nachrichten.

3. Wenn eine Nachricht einen Link zu einer Website enthält, klicken Sie nicht auf den Link. Suchen Sie stattdessen selbst online nach der Website, oder verwenden Sie die offizielle App.

4. Antworten Sie nicht auf eine Textnachricht unter der angegebenen Telefonnummer.

5. Rufen Sie die Organisation oder Person unter einer Telefonnummer zurück, die Sie selbst gefunden haben, z. B. auf der Website der Organisation.

E-Mail-Scamming

Scammer versenden E-Mails, die vorgeblich von einer staatlichen Stelle, Strafverfolgungsbehörden oder Unternehmen stammen. Sie lassen diese dringend klingen, um Sie zum schnellen Handeln zu bewegen.

Scammer verwenden das gleiche Logo und eine ähnliche E-Mail-Adresse wie die echte Organisation. Scammer können auch ihre E-Mail-Adresse hinter der E-Mail-Adresse einer Organisation oder eines Unternehmens kopieren oder verschleiern, um die betrügerische E-Mail echter aussehen zu lassen.

Anzeichen, dass eine E-Mail Scamming sein könnte

Die E-Mail:

Enthält eine Zahlungsaufforderung, aber die Kontodaten sind neu oder haben sich seit der letzten Zahlung geändert

Fordert Sie auf, sich mit Ihrem Benutzernamen und Passwort bei einem Online-Konto anzumelden oder andere persönliche Daten anzugeben

Ist unerwartet und enthält einen Anhang mit einer Aufforderung, diesen zu öffnen

Fordert Sie auf, Ihre Bankdaten zu bestätigen, um eine Rückerstattung oder Geld zu erhalten, das Sie nicht erwarten

Behauptet, Informationen über Sie oder Bilder von Ihnen zu haben, und droht damit, diese zu veröffentlichen

Bietet an, Ihnen zu helfen, Geld zurückzubekommen oder eine Entschädigung für eine Datenverletzung oder einen Identitätsdiebstahl zu erhalten

Maßnahmen, die Sie ergreifen können, um sich vor E-Mail-Scamming zu schützen

1. Prüfen Sie, ob die E-Mail echt ist, indem Sie entweder:
   a. die betreffende Person oder Organisation direkt unter Kontaktdaten kontaktieren, die Sie selbst gefunden haben, z. B. auf der Website der Organisation, oder
   b. auf eine Organisation über deren offizielle App zugreifen (niemals über einen Link).

2. Brechen Sie den Kontakt zu einer Person, die versucht, Sie zu bedrohen oder einzuschüchtern, sofort ab.

3. Geben Sie niemals persönliche Daten an und bezahlen Sie niemanden, der Ihnen Folgendes anbietet:
   a. Entschädigung oder Hilfe, um Ersatz für Schäden aus einem früheren Betrug oder einer Datenverletzung zu erlangen, oder
   b. Gewinne, Preise oder eine Erbschaft.

4. Verwenden Sie, wo immer möglich, eine mehrstufige Authentifizierung. Diese bietet Ihnen zusätzlichen Schutz und bedeutet, dass ein Scammer Ihr E-Mail-Passwort und eine an Ihr Telefon gesendete PIN kennen muss, um Zugang zu Ihrem E-Mail-Konto zu erhalten.

Telefon-Scamming

Scammer geben bei Anrufen vor, zu einer bekannten Organisation zu gehören. Dazu zählen staatliche Organisationen, Strafverfolgungsbehörden, Investment- und Anwaltsfirmen, Banken und Telekommunikationsanbieter.

Sie lassen diese Anrufe dringend klingen, um Sie zum schnellen Handeln zu bewegen. Sie versuchen möglicherweise, Sie zu überreden, ihnen Ihre persönlichen oder Bankkontodaten oder Zugang zu Ihrem Computer zu geben.

Der Anrufer kennt möglicherweise bereits einige Ihrer Details, z. B. Ihren Namen oder Ihre Adresse, so dass der Anruf echt erscheint.

Anzeichen dafür, dass ein Anruf Scamming sein könnte

Der Anrufer/die Anruferin:

Fordert Sie zu einer Zahlung auf oder bittet Sie, Geld auf ein neues Konto zu überweisen

Fragt Sie nach Ihrem Passwort, Ihrer PIN, einem Einmalcode oder anderen Sicherheitsinformationen

Fragt Sie nach Ihren Finanzdaten, z. B. Kreditkarten- oder Bankdaten

Fordert Sie auf, eine Aktion auf Ihrem Mobiltelefon oder Computer durchzuführen, z. B. eine Software zu installieren oder auf ein sicheres Konto zuzugreifen

Behauptet, von einer Strafverfolgungsbehörde zu sein, und droht Ihnen mit sofortiger Verhaftung oder Abschiebung

Sagt, dass Ihre Bank- oder anderen Online-Konten gehackt wurden oder in Betrug verwickelt sind

Maßnahmen, die Sie ergreifen können, um sich vor Telefon-Scamming zu schützen

1. Prüfen Sie, ob der Anruf echt ist, indem Sie entweder:
   a. die betreffende Person oder Organisation direkt unter Kontaktdaten kontaktieren, die Sie selbst gefunden haben, z. B. auf der Website der Organisation, oder
   b. auf eine Organisation über deren offizielle App zugreifen (niemals über einen Link).

2. Wenn Sie sich nicht sicher sind, wer der Anrufer ist, oder wenn ein Anrufer Sie bedroht oder einschüchtert, legen Sie sofort auf.

3. Installieren Sie niemals Software, die jemandem den Zugriff auf Ihren Computer oder Ihr Gerät ermöglicht.

4. Sie können Anrufe von Nummern, die Sie nicht kennen, ignorieren oder an Ihre Voicemail weiterleiten.

Gut zu wissen!

Sie können Scamming-Anrufe auch dann erhalten, wenn Ihre Rufnummer nicht öffentlich verzeichnet oder im „Do Not Call“-Register eingetragen ist.

Website-Scamming

Scammer können sich im Internet als eine beliebige Person ausgeben, einschließlich als Mitarbeitende einer staatlichen Stelle oder eines echten Unternehmens, als Prominente oder als Freund oder Familienmitglied.

Sie können gefälschte Websites erstellen, die wie die Websites bekannter Marken aussehen. Sie können sich als prominente Personen ausgeben und den Anschein erwecken, dass diese bestimmte Produkte oder Dienstleistungen unterstützen. Solche Websites können gefälschte Bewertungen enthalten, damit Sie ihnen vertrauen.

Möglicherweise sehen Sie online gefälschte Werbebanner oder Pop-up-Fenster, die gefälschte Warnungen oder Fehlermeldungen enthalten.

Anzeichen, dass eine Website Scamming sein könnte

Die Website:

Bietet Artikel zum Verkauf zu deutlich niedrigeren Preisen als üblich oder im Vergleich zu anderen Websites an

Bietet Informationen, wie Sie mit geringem Risiko und wenig Aufwand schnell und einfach Geld verdienen können

Enthält eine dringende Warnung oder Fehlermeldung, die Sie auffordert, auf einen Link zu klicken

Fordert Sie zu ungewöhnlichen oder speziellen Zahlungen auf, z. B. mit Geschenkkarten oder Kryptowährungen wie Bitcoin

Enthält nur positive Bewertungen

Maßnahmen, die Sie ergreifen können, um Website-Scamming zu vermeiden

1. Vergleichen Sie Preise. Angebote, die zu schön sind, um wahr zu sein, haben im Allgemeinen einen Haken.

2. Informieren Sie sich über die Organisation oder Person, mit der Sie zu tun haben, bevor Sie Geld zahlen oder Ihre persönlichen Daten weitergeben.

3. Verlassen Sie sich nicht auf Bewertungen auf der Website selbst. Suchen Sie die Website oder den Firmennamen und das Wort „Scam“ oder „Reviews“ bzw. „Bewertungen“.

4. Wenn auf Ihrem Bildschirm eine Warn- oder Fehlermeldung erscheint, klicken Sie nicht darauf, sondern gehen Sie direkt zu der Anwendung, auf die sie sich bezieht, um zu prüfen, ob sie echt ist.

5. Halten Sie das Gerät, das Sie zum Online-Shopping verwenden, auf dem neuesten Stand, indem Sie automatische Updates für Ihr Betriebssystem und Ihre Anwendungen aktivieren.

Gut zu wissen!

Praktische Möglichkeiten, sich online zu schützen, finden Sie unter www.cyber.gov.au

Scamming auf sozialen Medien, auf der Basis von Apps und Online-Nachrichtendiensten

Wenn Unbekannte Sie über soziale Medien, eine Messaging-Plattform wie WhatsApp oder WeChat oder über eine App kontaktieren, könnte es sich dabei um Scamming handeln.

Scammer, die sich als eine andere Person ausgeben, verwenden oft das echte Foto der Person oder das offizielle Logo der vorgegebenen Organisation, um den Betrug besser zu verschleiern.

Scammer erstellen in sozialen Medien gefälschte Profile und geben sich als Mitarbeitende staatlicher Stellen, eines echten Unternehmens, eines Arbeitgebers, einer Investmentfirma oder sogar als Freund, Familienmitglied oder möglicher Partner aus.

Sie geben sich eventuell auch als eine prominente Person aus, die scheinbar für ein Produkt oder eine Dienstleistung wirbt.

Scammer können auch aus den Informationen, die Sie über Ihre Konten in den sozialen Medien teilen, eine Menge über Sie erfahren. Sie können diese Informationen nutzen, um Ihre Passwörter für Ihre Konten zu erraten oder Sie mit anderen Betrügereien zu belästigen.

Anzeichen für Scamming über soziale Medien oder Apps

Das Profil im sozialen Medium oder die App:

Bietet Informationen, wie Sie mit geringem Risiko und wenig Aufwand schnell und einfach Geld verdienen können

Lädt Sie zur Teilnahme an einem Wettbewerb oder einem zeitlich begrenzten Angebot ein

Fordert Sie auf, eine Unterhaltung von einer App, z. B. einer Dating-App, in einen privaten Chat oder einen E-Mail-Verlauf zu verschieben

Suggeriert, dass eine prominente Person ein Produkt oder eine Dienstleistung befürwortet oder unterstützt

Gibt vor, dass jemand etwas, das Sie verkaufen, ohne vorherige Inspektion zu einem hohen Preis kaufen möchte

Droht damit, ein privates Bild von Ihnen zu veröffentlichen, wenn Sie kein Geld zahlen

Kontaktiert Sie, um Ihnen eine Stelle anzubieten

Gut zu wissen!

Informationen darüber, wie man sich auf verschiedenen sozialen Medienplattformen sicher verhält, finden Sie unter www.esafety.gov.au.

Maßnahmen, die Sie ergreifen können, um Scamming über soziale Medien und Apps zu vermeiden

1. Prüfen Sie, ob das Profil gefälscht sein könnte. Ist das Konto aktiv? Wie viele Freunde/Follower hat es und wie viel posten diese online?

2. Suchen Sie den Namen des Profils online zusammen mit dem Wort „Scam“.

3. Nehmen Sie niemals eine angebotene Stelle an, ohne ein Vorstellungsgespräch oder ein Gespräch über Ihre Erfahrung, Eignung und Referenzen geführt zu haben. Recherchieren Sie den Personalvermittler und die Organisation oder Person, die die Stelle anbietet. Setzen Sie sich mit dem Personalvermittler über eine Telefonnummer in Verbindung, die Sie bei einer unabhängigen Internetrecherche ermittelt haben. Zahlen Sie kein Geld im Voraus, nur um sich eine Stelle zu sichern.

4. Lassen Sie sich zu möglichen Investitionen nur von Personen beraten, die über eine Lizenz als australischer Finanzdienstleister verfügen, und vergewissern Sie sich, dass ein Unternehmen oder eine Website nicht auf dem Anlegerwarnportal der International Organization of Securities Commission (IOSCO) aufgeführt ist.

5. Zahlen Sie niemals einer Person Geld, die Sie nur online kennengelernt haben. Scammer behaupten oft, dass sie im Ausland leben und Sie nicht persönlich kennenlernen können.

6. Senden Sie niemals einer Person, die Sie nur online kennengelernt haben, intime Bilder von sich.

Weitere Informationen über Scamming-Maschen und andere Möglichkeiten der Kontaktaufnahme durch Scammer, z. B. persönlich oder per Post, finden Sie bei Scamwatch.

Die wichtigsten Scamming-Maschen, die Sie kennen sollten

Hier sind einige der häufigsten Scamming-Maschen, die Sie kennen sollten. Auf der Scamwatch-Website finden Sie weitere Informationen über die verschiedenen Methoden, einschließlich Warnzeichen und Schutzmaßnahmen.

Scamming durch Identitätsbetrug

Scammer gaukeln Ihnen vor, sie kämen von einer vertrauenswürdigen Organisation wie der Polizei, einer staatlichen Stelle, einer Bank oder einem bekannten Unternehmen. Sie geben möglicherweise sogar vor, ein Freund oder Familienmitglied zu sein. Scammer suchen nach Informationen über Sie, indem sie Phishing-E-Mails oder -Nachrichten versenden. Diese sind darauf ausgelegt, Ihre Daten zu stehlen. Sie versuchen, Sie zur Herausgabe persönlicher Daten zu überzeugen, indem sie vortäuschen, von einer offiziellen Organisation zu kommen oder jemand zu sein, den Sie kennen und dem Sie vertrauen.

Scammer nutzen Technologien, um ihre Anrufe oder Nachrichten so aussehen zu lassen, als kämen sie von einer legitimen Telefonnummer. Sie können Textnachrichten im gleichen Gesprächsverlauf wie echte Nachrichten eines Unternehmens erscheinen lassen.

Geldanlage-Scamming

Scammer nutzen überzeugendes Marketing und neue Technologien, damit ihr Investitionsangebot einfach zu gut klingt, um es zu verpassen. Sie versprechen Ihnen hohe Dividenden bei geringem oder gar keinem Risiko. Sie setzen Sie oft unter Druck, um Sie zu schnellem Handeln zu bewegen, damit sie Ihr Geld stehlen können.

Job- und Beschäftigungs-Scamming

Scammer bieten Stellen an, die gut bezahlt werden und wenig Aufwand erfordern. Sie geben vor, im Auftrag von namhaften Unternehmen und Online-Shopping-Plattformen Personen einzustellen. Manchmal gibt es die ausgeschriebene Stelle gar nicht. Scammer geben sich auch als bekannte Personalvermittlungsagenturen aus. Ihr Ziel ist es, Ihr Geld und Ihre persönlichen Daten zu stehlen. Möglicherweise fordern sie Sie zu einer Vorauszahlung auf, damit Sie für sie arbeiten können.

Produkt- und Dienstleistungs-Scamming

Scammer geben sich als Käufer oder Verkäufer aus, um Ihr Geld zu stehlen. Sie erstellen gefälschte Websites oder Profile auf Websites seriöser Einzelhändler, die Produkte oder Dienstleistungen zu Preisen anbieten, die zu gut sind, um wahr zu sein. Sie veröffentlichen gefälschte Anzeigen und falsche Bewertungen. Sie verwenden möglicherweise gestohlene Logos, einen .com.au-Domainnamen und/oder eine gestohlene australische Firmennummer (ABN). Diese Scamming-Maschen sind schwer zu erkennen.

Scammer geben sich auch als Unternehmen aus, die Sie kennen und denen Sie vertrauen, um Ihnen gefälschte Rechnungen zu schicken. Sie können sogar Details auf legitimen Rechnungen ändern, so dass Kunden letztendlich den Scammer statt Sie bezahlen.

Romantik-Scamming

Scammer nutzen das Versprechen von Liebe, Verabredungen oder Freundschaft, um Ihr Geld zu stehlen. Sie geben sich große Mühe, Sie davon zu überzeugen, dass die Beziehung echt ist, und manipulieren Sie, damit Sie ihnen Geld geben.

Scammer finden Sie über soziale Medien, Dating- oder Spiele-Apps und Websites. Möglicherweise senden sie Ihnen auch eine SMS oder E-Mail. Sie verstecken sich hinter gefälschten Profilen und Identitäten, manchmal von berühmten Personen. Sobald Sie der Person vertrauen, tritt bei ihr ein „Notfall“ ein, und Sie werden um Hilfe gebeten. Dabei handelt es sich oft um Bitten um Geld oder andere Produkte.

Drohungs- und Erpressungs-Scamming

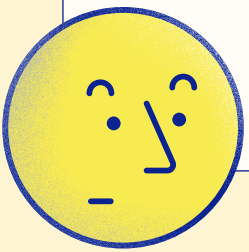
Scammer geben sich als Mitarbeitende einer vertrauenswürdigen Organisation aus und behaupten, Sie müssten Geld zahlen, sonst würde etwas Schlimmes passieren. Sie drohen Ihnen möglicherweise mit Verhaftung, Abschiebung oder sogar körperlicher Gewalt, wenn Sie nicht sofort zahlen.

Sie können Sie auch erpressen, indem sie damit drohen, Nacktbilder oder Videos, die Sie ihnen geschickt haben, weiterzugeben, wenn Sie ihnen kein Geld schicken.

Scamming mit unerwartetem Geld

Scammer versuchen, Sie davon zu überzeugen, dass Ihnen Geld oder Gewinne zustehen, mit deren Erhalt Sie nicht gerechnet haben.

Sie fordern Sie dann auf, eine Gebühr zu zahlen oder Ihre Bank- oder Identitätsdaten anzugeben, bevor Sie das Geld oder den Gewinn in Empfang nehmen können. Doch leider gibt es dabei kein geschenktes Geld.



Wo können Sie Scamming melden?

Wir arbeiten daran, Scamming in Australien zu erschweren, indem wir das Bewusstsein dafür schärfen, wie man es erkennen, vermeiden und melden kann.

Wir tauschen Informationen aus Scamming-Meldungen aus und arbeiten mit staatlichen Stellen, Strafverfolgungsbehörden und dem privaten Sektor zusammen, um Scamming zu unterbinden und ihm vorzubeugen.

Helfen Sie anderen, indem Sie Scamming an Scamwatch melden. Melden Sie Ihre Scamming-Erfahrung über das Meldeformular auf der Scamwatch-Website unter www.scamwatch.gov.au.

Denken Sie daran: Wenn Sie Opfer von Scamming geworden sind, ist es wichtig, schnell zu handeln.

- Wenn Sie Geld an einen Scammer verloren haben, wenden Sie sich an Ihre Bank oder Ihren Kartenanbieter.
- Wenden Sie sich an ID CARE: 1800 595 160 | idcare.org

Weitere Hilfe und Unterstützung

Opfer von Scamming geworden zu sein, kann überwältigen. Es ist wichtig, nicht zu vergessen, dass es jeden treffen kann und dass es Hilfe gibt.

Wenn Sie oder jemand, den Sie kennen, Opfer von Scamming geworden ist, sprechen Sie mit jemandem darüber. Wenden Sie sich sich an Ihre Familie, Freunde, Ihren Hausarzt oder einen der folgenden Dienste.

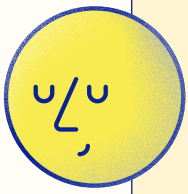
Lifeline: 13 11 14 | lifeline.org.au
oder den Online-Krisenhilfe-Chat (24 Stunden am Tag, 7 Tage die Woche)

Beyond Blue: 1300 22 4636 | beyondblue.org.au
oder den Online-Chat (24 Stunden am Tag, 7 Tage die Woche)

Kids Helpline: 1800 55 1800 | kidshelpline.com.au
(24 Stunden am Tag, 7 Tage die Woche)

Die finanziellen Auswirkungen von Scamming können verheerend und lebensverändernd sein.

Wenn Sie sich in einer finanziellen Notlage befinden, können Sie über die National Debt Helpline mit einem Finanzberater sprechen: 1800 007 007 montags bis freitags von 9:30 – 16:30 Uhr oder nutzen Sie den Live Chat montags bis freitags von 9:00 – 20:00 Uhr



scamwatch.gov.au