



**Sicher
unterwegs
im Internet**

Vorwort

Die Aufgabe der Polizei ist es, die bestmögliche Sicherheit für die Bevölkerung zu gewährleisten. Die intensive Zusammenarbeit mit verschiedenen Partnerorganisationen und dem Land NÖ wirkt sich dabei besonders positiv aus.

Im Feld der Computer- und Internetkriminalität sind diese Zusammenarbeit und damit verbunden die Information der Bevölkerung über aktuelle kriminelle Praktiken und Verhaltenstipps von eminenter Bedeutung.

Seit mehreren Jahren ist im Bereich der Online-Kriminalität ein stetiges Wachstum zu beobachten. Auch die Pandemie führte, im Unterschied zu anderen Kriminalitätsfeldern, im Bereich der Computer- und Internetkriminalität nicht zu einer Abschwächung.

Auf den folgenden Seiten können Sie aktuelle Informationen finden und Tipps nachlesen. Speziell ausgebildete Expertinnen und Experten der Kriminalprävention im Bereich Computer- und Internetkriminalität informieren Sie aber auch gerne bei Einzelberatungen oder Vorträgen.

Ich wünsche Ihnen alles Gute und freue mich auf eine weitere gute Zusammenarbeit.

Franz Popp, BA, MA

Landespolizeidirektor Niederösterreich





Vorwort

In einer zunehmend digitalisierten Welt ist die Sicherheit im Internet von größter Bedeutung. Diese Informationsbroschüre soll Ihnen nicht nur wertvolle Tipps und Hinweise zur sicheren Nutzung des Internets geben, sondern auch spezifische Informationen zur Sicherheit beim Internetbanking und bei Online-Überweisungen bieten.

Die Zusammenarbeit mit der Polizei ist ein wichtiger Schritt, um die Bedrohungen im digitalen Raum effektiv zu bekämpfen. Cyberkriminalität nimmt stetig zu, und es ist unser gemeinsames Anliegen, Sie als unsere Kundinnen und Kunden bestmöglich zu schützen. Ein zentraler Aspekt unserer Sicherheitsstrategie sind daher die kontinuierliche Schulung und Sensibilisierung unserer Mitarbeiterinnen und Mitarbeiter. Nur durch ein hohes Maß an Bewusstsein und Wissen können wir gemeinsam gegen Cyberkriminalität vorgehen. In dieser Broschüre erfahren Sie, wie Sie selbst aktiv zur Sicherheit beitragen können, indem Sie beispielsweise starke Passwörter verwenden, verdächtige E-Mails erkennen und sichere Verbindungen nutzen.

Sicherheit im Internet ist unsere gemeinsame Aufgabe. Nur durch die enge Zusammenarbeit zwischen allen Beteiligten können wir ein sicheres digitales Umfeld schaffen. Ich lade Sie daher ein, die Informationen in dieser Broschüre aufmerksam zu lesen und die empfohlenen Sicherheitsmaßnahmen in Ihrem Alltag umzusetzen.

Wolfgang Viehauser

HYPO NOE Vorstand





Grundlegende Sicherheitshinweise

Im Internet wird die Anonymität häufig von Kriminellen ausgenutzt, um betrügerische Taten zu begehen. Daher ist es wichtig, beim Surfen im World Wide Web besonders vorsichtig zu sein. Um sicher online unterwegs zu sein und Ihre Anonymität zu schützen, sollten Sie einige grundlegende Tipps beachten, um nicht Opfer von Betrügern zu werden. Oft versuchen Betrüger, Internetnutzer mit professionell aussehenden Inhalten oder durch gezielte Verunsicherung zu täuschen.

Die folgenden Tipps stellen wichtige Mindestanforderungen für eine sichere Nutzung des Internets dar:

SCHÜTZEN SIE IHREN COMPUTER VOR VIREN UND MALWARE

Stellen Sie sicher, dass auf Ihrem Computer ein Virenschutzprogramm sowie eine Firewall installiert sind. Achten Sie darauf, dass diese regelmäßig aktualisiert werden. Es ist ratsam, automatische Updates für Ihre Sicherheitssoftware zu aktivieren.

VERWENDEN SIE STARKE PASSWÖRTER

Schützen Sie Ihren Computer, Ihre E-Mail-Konten und alle weiteren Online-Accounts mit sicheren Passwörtern. Ein gutes Passwort sollte mindestens 12 Zeichen umfassen und eine Mischung aus Groß- und Kleinbuchstaben, Zahlen sowie Sonderzeichen enthalten.

→ **Beispiel:** Merken Sie sich **95** Sätze und nutzen Sie nur die Anfangsbuchstaben der Wörter:

→ **Passwort:** #MSs95SunSndAdW+

Ihrer Kreativität sind keine Grenzen gesetzt!

NUTZEN SIE PASSWORTMANAGER

Wenn nötig, können Sie auch Passwortmanager verwenden, um komplexe Passwörter zu erstellen und sicher zu speichern. In diesem Fall sind europäische Anbieter zu bevorzugen.

AKTIVIEREN SIE DIE ZWEI-FAKTOR-AUTHENTIFIZIERUNG (2FA)

Wo immer es möglich ist, sollten Sie die Zwei-Faktor-Authentifizierung aktivieren, um eine zusätzliche Sicherheitsebene für Ihre Online-Konten hinzuzufügen.

SICHERN SIE WICHTIGE DATEN REGELMÄSSIG

Erstellen Sie Backups Ihrer wichtigen Daten auf externen Festplatten oder anderen Datenträgern, um im Falle eines Datenverlustes abgesichert zu sein.

VERMEIDEN SIE DIE NUTZUNG SENSIBLER DATEN IN ÖFFENTLICHEN WLAN-NETZWERKEN

Wenn Sie auf öffentliche WLANs angewiesen sind, sollten Sie ein VPN (Virtual Private Network) verwenden, um Ihre Internetverbindung zu verschlüsseln und Ihre Daten zu schützen.



Betrug im Internet

In der heutigen digitalen Welt ist das Internet zu einem unverzichtbaren Bestandteil unseres Lebens geworden. Doch während das World Wide Web viele Vorteile bietet, birgt es auch Gefahren – insbesondere in Form von Betrug und kriminellen Machenschaften. Immer mehr Menschen fallen auf betrügerische Websites, Phishing-Mails und Online-Fallen herein.

Betrüger nutzen geschickt die Anonymität des Internets aus, um ahnungslose Nutzer zu täuschen und zu schädigen. Sei es durch vermeintlich unschlagbare Angebote, die zu gut erscheinen, um wahr zu sein, oder durch gefälschte Rechnungen, die ein Unternehmen vorgaukeln, das gar nicht existiert – der Fantasie der Täter sind keine Grenzen gesetzt. Auch Partnerbörsen und Online-Kontakte sind nicht vor betrügerischen Aktivitäten sicher. Besonders perfide sind die sogenannten „Love Scams“, bei denen sich Täter emotional an ihre Opfer binden, um sie später um Geld zu betrügen.

Deshalb ist es entscheidend, sich stets bewusst zu sein, dass nicht alles, was im Internet angeboten wird, auch tatsächlich vertrauenswürdig ist.

Es gibt jedoch einfache Maßnahmen, mit denen sich jeder effektiv vor Internetbetrug schützen kann:

VORSICHT BEI UNREALISTISCHEN ANGEBOTEN

Wenn eine Website oder eine E-Mail eine Leistung zu sehr niedrigen Preisen oder sogar kostenlos anbietet, handelt es sich oft um einen Betrugsversuch. Löschen Sie solche E-Mails sofort oder verlassen Sie die Website.

RECHNUNGEN ÜBERPRÜFEN

Wenn Sie per E-Mail eine Rechnung erhalten, überlegen Sie, ob Sie wirklich bei diesem Unternehmen eine Bestellung aufgegeben haben. Falls nicht, löschen Sie die E-Mail sofort und öffnen Sie auf keinen Fall den Anhang – dieser könnte ein Virus enthalten. Bei Unsicherheiten rufen Sie die offizielle Telefonnummer des Unternehmens an.

BEHÖRDEN-E-MAILS

Behörden verschicken niemals E-Mails, es sei denn, Sie haben zuvor zugestimmt. E-Mails, die wie offizielle Mitteilungen aussehen und Logos von Behörden, Unternehmen oder Anwälten enthalten, können gefälscht sein. Lassen Sie sich nicht unter Druck setzen und rufen Sie im Zweifelsfall die offizielle Telefonnummer der Behörde oder des Unternehmens an.

BEKANNTE ANBIETER WÄHLEN

Wenn Sie Waren online kaufen, bevorzugen Sie bekannte Anbieter oder Händler, denen Sie vertrauen.

VORSICHT BEI IDENTITÄTSDOKUMENTEN

Vermeiden Sie Online-Shops, die nach Kopien von Identitätsdokumenten oder Kreditkartendaten fragen – dies könnte auf den Versuch eines Identitätsdiebstahls hindeuten.

PREISVERGLEICHE NUTZEN

Vergleichen Sie Preise vor dem Einkaufen mithilfe von Preisvergleichsportalen. Wenn die Preise zu günstig erscheinen, sollten Sie lieber woanders kaufen – möglicherweise handelt es sich um einen Fakeshop.

ÜBERPRÜFEN SIE FAKESHOPS

Informieren Sie sich auf Websites wie www.watchlist-internet.at, ob es sich um einen Fakeshop handelt, oder wenden Sie sich an den Konsumentenschutz, wenn Sie Zweifel haben.

BANKGESCHÄFTE SICHER DURCHFÜHREN

Nutzen Sie niemals einen Link in einer E-Mail oder auf einer Website, um sich in Ihr Bankkonto einzuloggen. Tippen Sie die Internetadresse der Bank direkt in den Browser ein. Eine sichere Website erkennt man an „https“ und einem Schlosssymbol in der Browserzeile.

SENSIBLE DATEN SCHÜTZEN

Geben Sie keine sensiblen Informationen wie Bankdaten, Passwörter oder Kreditkarteninformationen über das Internet oder per E-Mail weiter. Seriöse Unternehmen verlangen solche Informationen nicht.

VORSICHT BEI ONLINE-PARTNERBÖRSEN

Seien Sie besonders vorsichtig, wenn eine Online-Bekannntschaft Geld fordert, emotionalen Druck ausübt oder Sie zu sexuellen Handlungen auffordert. Übermitteln Sie keine persönlichen Fotos oder Videos, da diese für Erpressung genutzt werden könnten.

GELDÜBERWEISUNGEN AN INTERNETBEKANNTSCHAFTEN VERMEIDEN

Überweisen Sie niemals Geld an Personen, die Sie ausschließlich aus dem Internet kennen – häufig handelt es sich um Betrug.

PRÜFEN SIE DIE QUELLE VON INFORMATIONEN

Seien Sie besonders vorsichtig bei Inhalten, die Sie nicht überprüfen können. Fake News, betrügerische Websites und manipulative Werbung können Sie leicht in die Irre führen.

SEIEN SIE VORSICHTIG BEI LINKS UND ANHÄNGEN

Klicken Sie nicht auf verdächtige Links und öffnen Sie keine unbekannten Anhänge, insbesondere aus E-Mails oder Nachrichten, die Sie nicht erwartet haben.



Sichere Nutzung von Social Media

PRIVATSPHÄRE-EINSTELLUNGEN ANPASSEN

Überprüfen Sie regelmäßig die Datenschutzeinstellungen Ihrer Social-Media-Konten und stellen Sie sicher, dass nur vertrauenswürdige Personen Zugriff auf Ihre persönlichen Informationen und Beiträge haben. Begrenzen Sie die Sichtbarkeit Ihrer Beiträge auf „Freunde“ oder „Bekannte“, wenn möglich.

SEIEN SIE VORSICHTIG MIT PERSÖNLICHEN INFORMATIONEN

Geben Sie keine sensiblen Informationen wie Ihre Adresse, Telefonnummer oder finanzielle Details in öffentlichen Posts oder Nachrichten preis. Seien Sie sich bewusst, dass diese Informationen von Dritten missbraucht werden könnten.

STARKE PASSWÖRTER VERWENDEN UND 2FA AKTIVIEREN

Nutzen Sie starke, einzigartige Passwörter für jedes Social-Media-Konto und aktivieren Sie, wenn möglich, die Zwei-Faktor-Authentifizierung (2FA) für zusätzlichen Schutz. Diese Sicherheitsmaßnahme hilft, unbefugten Zugriff auf Ihre Konten zu verhindern.

VORSICHT BEI UNBEKANNTEN KONTAKTEN UND LINKS

Akzeptieren Sie keine Freundschaftsanfragen von Unbekannten und klicken Sie nicht auf verdächtige Links oder Anhänge, die von fremden oder zweifelhaften Konten stammen. Phishing-Angriffe sind eine häufige Methode, um persönliche Daten zu stehlen.

SEIEN SIE ACHTSAM BEI APPS UND BERECHTIGUNGEN

Überprüfen Sie regelmäßig, welche Apps oder Drittanbieter auf Ihre Social-Media-Konten zugreifen können, und entziehen Sie unnötige Berechtigungen. Stellen Sie sicher, dass Sie nur vertrauenswürdigen Anwendungen Zugriff gewähren.

FÜGEN SIE KEINE FREMDEN PERSONEN IHRER FREUNDESLISTE HINZU

Prüfen Sie genau, wen Sie als Freund bzw. Follower akzeptieren, es könnte sich um Betrüger handeln.

VORSICHT BEI CHATS BZW. VIDEOTELEFONIE MIT SEXUELLEM HINTERGRUND

Häufig handelt es um Kriminelle, die Ihre Opfer mit Videoaufnahmen erpressen wollen.



Achtung Investmentbetrug

Investmentbetrug oder Anlagebetrug ist eine Form des Betrugs, bei der Betrüger versuchen, Anleger dazu zu bringen, Geld in nicht existente oder wertlose Anlagen zu investieren. Tatort ist auch hier häufig das Internet. Die Betrüger nutzen oft folgende Methoden:

FALSCHES VERSPRECHEN

Betrüger locken Anleger mit unrealistisch hohen Renditen und schnellen Gewinnen. Sie präsentieren ihre Angebote oft als „einmalige Gelegenheit“.

DRINGLICHKEIT UND DRUCK

Oft wird ein Gefühl der Dringlichkeit erzeugt, um Anleger zu schnellen Entscheidungen zu drängen. Sätze wie „Das Angebot gilt nur für kurze Zeit“ sind häufig.

FALSCHES IDENTITÄTEN

Betrüger geben sich häufig als vertrauenswürdige Finanzberater oder Vertreter bekannter Unternehmen aus, um Glaubwürdigkeit zu gewinnen.

KOMPLEXE STRUKTUREN

Die Angebote sind oft kompliziert und schwer verständlich, was es den Anlegern erschwert, die Risiken zu erkennen.

UNREGULIERTE MÄRKTE

Viele Betrüger operieren in unregulierten Märkten oder über Off-shore-Unternehmen, was die Rückverfolgbarkeit erschwert.

Um nicht Opfer eines Anlagebetruges zu werden, sollten Sie folgende Tipps beachten:

RECHERCHIEREN SIE GRÜNDLICH

Überprüfen Sie die Identität des Anbieters und die angebotenen Anlagen. Suchen Sie nach Bewertungen, Erfahrungsberichten und regulatorischen Informationen.

MISSTRAUEN SIE UNREALISTISCHEN RENDITEN

Seien Sie skeptisch gegenüber Angeboten, die hohe Renditen mit geringem Risiko versprechen. Hohe Gewinne sind oft mit hohen Risiken verbunden.

LASSEN SIE SICH ZEIT

Nehmen Sie sich Zeit, um Entscheidungen zu treffen. Dringlichkeit ist oft ein Zeichen für Betrug.

ACHTEN SIE AUF WARNSIGNALE

Seien Sie vorsichtig bei Angeboten, die über soziale Medien, E-Mails oder Telefonanrufe beworben werden, insbesondere wenn sie unaufgefordert eintreffen.

SCHÜTZEN SIE IHRE PERSÖNLICHEN DATEN

Geben Sie keine sensiblen Informationen preis, es sei denn, Sie sind sicher, dass der Anbieter legitim ist.



Sicherheit beim Internetbanking

ZUGRIFF PRÜFEN

Stellen Sie sicher, dass ausschließlich vertrauenswürdige Personen Zugriff auf die Administration Ihrer Computer und Mobilgeräte haben. Vermeiden Sie es, Bankgeschäfte auf fremden oder unsicheren Geräten durchzuführen. Meiden Sie auch freie und ungesicherte WLAN-Hotspots für Ihre Online-Bankgeschäfte.

SYSTEME IMMER AKTUELL HALTEN

Nutzen Sie ausschließlich Geräte mit einem aktuellen, sicherheitsoptimierten Betriebssystem. Veraltete Betriebssysteme können erhebliche Sicherheitslücken aufweisen und bieten Cyberkriminellen sowie Schadsoftware eine leichte Angriffsfläche.

VORSICHT VOR FREMD-PROGRAMMEN

Installieren Sie keine Programme auf Ihrem Computer und keine Apps auf Ihrem Mobilgerät, die Ihnen unerwartet empfohlen werden, etwa in einer E-Mail, einer SMS oder in einem Telefongespräch. Installieren Sie kein Fernwartungs-Tools auf Ihrem Computer und erlauben Sie keiner Ihnen unbekannten Person einen Fernzugriff auf Ihren

Computer. Auch dann nicht, wenn diese Person vorgibt, Support-Mitarbeiter:in von einem bekannten Unternehmen (Microsoft, Hausbank etc.) zu sein.

Laden Sie Apps nur aus den offiziellen App-Stores (Apple App Store, Google Play Store) auf Ihr Mobilgerät. Sollten Apps bei der Installation Berechtigungen anfordern, die nicht nachvollziehbar sind oder unnötig erscheinen, brechen Sie die Installation ab bzw. löschen Sie diese Apps umgehend.

ZUGANGSDATEN VERTRAULICH BEHANDELN

Behandeln Sie persönliche geheime Zugangsdaten, Codes, Passwörter sowie Konto- und Kartendaten stets vertraulich und geben Sie diese niemals an Dritte weiter – nicht auf Anfrage in einer Nachricht und auch nicht, wenn Sie in einem Telefongespräch dazu aufgefordert werden. Seriöse Unternehmen wie z.B. Ihre Hausbank verschicken niemals E-Mails oder SMS und fordern auch niemals in einem Telefongespräch die Herausgabe sensibler Daten.

HYPO NOE ID APP EINSETZEN

Prüfen Sie jede Anforderung zu einem Login oder einer Transaktion (Überweisung) sorgfältig, bevor Sie das Login ins Internetbanking oder den Zahlungsauftrag zur Durchführung in der HYPO NOE ID App freigeben. Vergewissern Sie sich immer, dass die in der ID App zur Freigabe angezeigten Informationen mit den zuvor im Internetbanking oder in der Banking App eingegebenen Daten übereinstimmen.

Geben Sie keinen Login in Ihr Internetbanking frei und autorisieren Sie keinen Auftrag in der HYPO NOE ID App, wenn Sie diese nicht zuvor selbst in Ihrem Internetbanking oder Ihrer Banking App initiiert haben. Wichtig: Um Geld zu erhalten, ist niemals eine Bestätigung oder Freigabe erforderlich.

Beachten Sie die Empfehlungen und aktuelle Informationen Ihrer Hausbank für die sichere Nutzung des Internetbankings.

IMPRESSUM

Medieninhaber: Landeskriminalamt NÖ - Kriminalprävention
3100 St. Pölten, Schanze 7 | Verlagsort: St. Pölten

Hersteller und Herstellungsort: Print Alliance HAV Produktions GmbH, Druckhausstraße 1, A-2540 Bad Vöslau
Layout: Florian Herndl, flosse.at | Fotos: Adobe Stock, zVg

in Kooperation mit: HYPO NOE Landesbank für Niederösterreich und Wien AG,
Hypogasse 1, 3100 St. Pölten

Alle Recherchen wurden sorgfältig durchgeführt, sind aber ohne Gewähr. Haftungsansprüche sind ausgeschlossen. Stand: Juni 2025. Soweit personenbezogene Bezeichnungen nur in männlicher Form angeführt sind, beziehen sie sich auf Frauen und Männer in gleicher Weise.



HYPO NOE



