Senioren im Internet – Aber sicher!

60 Tipps und Hinweise für die sichere Internetnutzung

Landesrat für
Kriminalitätsvorbeugung
Mecklenburg-Vorpommern

1. Vorwort

Die Entwicklung des Internet ist in den vergangenen Jahren rasant vorangeschritten. Eine schier unerschöpfliche Menge an Informationen und Möglichkeiten bietet neue Freiheiten für Menschen jeden Alters. Ob Einkaufsbummel, Behördengang oder Bankgeschäft, im Internet lassen sich die Dinge des täglichen Lebens schnell und unkompliziert erledigen. Zudem wird vielfach der Kontakt zu Bekannten und Verwandten durch die neue Kommunikationstechnik erleichtert. Auch immer mehr ältere Bürgerinnen und Bürger nutzen das Internet. Denn gerade Seniorinnen und Senioren können von den kurzen elektronischen Wegen profitieren. Wie die altbekannte analoge Welt auch, ist diese neu entstandene virtuelle Welt aber nicht frei von Stolperfallen und Gefahren. Eine gesunde Skepsis und das Bauchgefühl können helfen, heikle Situationen zu erkennen. Die folgenden Tipps sollen Sie dabei unterstützen. Sie sollen aber zugleich ermutigen, die Chancen dieses neuen Mediums im Alltag zu nutzen, ohne die Sicherheit aus den Augen zu verlieren.

Diese von der Arbeitsgruppe Seniorensicherheit des Landesrates für Kriminalitätsvorbeugung zusammengestellten 60 Tipps konzentrieren sich ganz bewusst auf die aus unserer Sicht wichtigsten **10 Schwerpunkte**. Wenn Sie diese beachten, sind Sie gegen „Nepper – Schlepper – Bauernfänger" in der digitalen Welt gut gerüstet.

Wer sich darüber hinaus informieren möchte, findet zahlreiche weiterführende Hinweise auf den genannten Internetseiten.

2. 60 Tipps und Hinweise

2.1 Internetsicherheit allgemein

- Das Internet ist kein rechtsfreier Raum. Auch hier gelten Recht und Gesetz.
- Hüten Sie Ihre persönlichen Daten, so wie in der realen Welt.
- Das Internet hat ein langes Gedächtnis. Einmal eingestellt, sind Daten nur sehr schwer wieder zu entfernen.
- Machen Sie sich bewusst, dass Ihre persönlichen Daten für viele sichtbar und von Wert sind.
- Auch Sie hinterlassen mit einer Protokolladresse bei jeder Aktion im Internet Spuren.
- Niemand hat im Internet etwas zu verschenken, viele Dienste werden durch Werbung und Datennutzung finanziert.
- Widersprechen Sie der Nutzung Ihrer Daten zum Zweck der Werbung, Markt- und Meinungsforschung bei den Unternehmen.
- Beenden Sie nach vorherigem Anmelden eine Internetsitzung im Anschluss auch immer über die Abmeldefunktion.

2.2 Viren, Trojaner und unberechtigten Zugriff verhindern

- Installieren und aktualisieren Sie eine Virenschutzsoftware auf Ihrem Computer und starten Sie regelmäßig einen Suchlauf. Sie können diese für den privaten Gebrauch zum Teil kostenlos im Internet herunterladen. Darüber hinaus sind Programme mit umfangreicheren Diensten in der Regel kostenpflichtig zu beziehen.
- Aktualisieren Sie regelmäßig Ihr Betriebssystem und Ihren Internetbrowser (z. B.: Windows-Update, Windows-Explorer-Update), um Sicherheitslücken zu schließen, über die sonst ungehindert Schadsoftware eindringen könnte. Für eine zeitnahe Auffrischung des Schutzes ist es sinnvoll, automatische Update-Dienste zu nutzen.
- Schränken Sie den Zugriff auf Ihren Computer ein (Firewall, Benutzerkonten).

- Nutzen Sie Programme, die Sie vor unseriösen Internetseiten warnen.

2.3 Passwörter sichern

- Kombinieren Sie Passwörter mit Zahlen, Buchstaben und Sonderzeichen von mindestens 8 Stellen.
- Wählen Sie keine Passwörter aus dem Wörterbuch, Namen, Geburtsdaten oder einfache Zahlen- und Buchstabenfolgen.
- Bilden Sie zum Beispiel einen einprägsamen Satz und nutzen Sie die Anfangsbuchstaben der Wörter und die Satzzeichen als Passwort.
- Speichern Sie Passwörter keinesfalls auf dem Computer.
- Ein regelmäßiger Wechsel des Passwortes erhöht die Sicherheit.
- Verwenden Sie für verschiedene Zugänge keine einheitlichen Passwörter.

2.4 Einkauf mit Bedacht

- Bevorzugen Sie vertrauenswürdige Internetseiten, die Ihnen bekannt sind oder empfohlen wurden.
- Prüfen Sie die Allgemeinen Geschäftsbedingungen und das Impressum Ihnen unbekannter Anbieter.
- Achten Sie auf Zertifikate, Gütesiegel und Hinweise in Bewertungsportalen, um seriöse Anbieter zu finden.
- Überprüfen Sie bei Online-Auktionen das Profil Ihres potentiellen Vertragspartners.
- Beziehen Sie keine Medikamente von unseriösen Anbietern im Internet.
- Nutzen Sie verschlüsselte Verbindungen (auf https:// und Schlosssymbol in der Adresszeile achten) und bevorzugen Sie sichere Bezahlverfahren, wie Bankeinzug oder Rechnung.
- Informieren Sie sich auch über gebührenpflichtige, aber sichere Internetbezahlverfahren (z. B.: Paypal, Firstgate).

2.5 Sichere Bankgeschäfte

- Lassen Sie sich von Ihrer Bank zum sicheren Internetverkehr beraten.
- Schützen Sie Ihre Zugangsdaten sowie Transaktionsnummern (PIN und TAN) vor unberechtigtem Zugriff und speichern Sie diese nicht auf dem Computer.
- Prüfen Sie die Echtheit Ihrer Bank-Webseite und geben Sie die Internetadresse Ihrer Bank von Hand ein.
- Ignorieren Sie E-Mails, die Sie zur Eingabe Ihrer Kontodaten auffordern. Keine Bank würde Sie dazu veranlassen (Phishing = Passwörter abfischen).
- Vereinbaren Sie ein Limit für tägliche Geldbewegungen und sperren Sie Ihren Kontozugang, wenn Ihnen etwas verdächtig vorkommt.
- Verwenden Sie verschlüsselte Verbindungen und eine aktuelle Schutzsoftware, um Ausspähungen zu verhindern.

2.6 Vorsicht bei sozialen Netzwerken und Kontaktbörsen

- Lesen Sie zum Schutz Ihrer einzustellenden Daten die Allgemeinen Geschäftsbedingungen und Bestimmungen zum Datenschutz des Anbieters.
- Nutzen Sie unbedingt die angebotenen Privatisierungseinstellungen.
- Kommunizieren Sie zu Ihrer Sicherheit ausschließlich unter Pseudonym.
- Veröffentlichen Sie private Informationen, Texte und Bilder sehr zurückhaltend und in keinem Fall reale Anschriften und Erreichbarkeiten.
- Achten Sie bei der Auswahl des Netzwerkes auf seriöse Betreuung und Führung der Online-Gemeinschaft. Beziehen Sie die Erfahrungen Ihnen bekannter Nutzer ein.
- Seien Sie skeptisch gegenüber Kontaktanfragen Ihnen unbekannter Personen.

- Melden Sie aufdringliche Kontakte dem Betreiber des Netzwerkes.
- Seien sie äußerst misstrauisch, wenn Online-Bekannte Sie um Geld oder andere Leistungen bitten.

2.7 Sichere elektronische Post

- Geben Sie Ihre E-Mail-Adresse nur an vertrauenswürdige Personen weiter und öffnen Sie auch scheinbar ungefährliche Dateianhänge nie ungeprüft. Fragen Sie beim Absender nach, sollten Sie unsicher sein.
- Seien Sie insbesondere sorgsam im Umgang mit eingehenden E-Mails Ihnen unbekannter Absender und öffnen Sie nicht deren Dateianhänge (Gefahr des Einschleusens von Schadprogrammen).
- Werden Sie bei E-Mails mit Schlagwörtern, wie „Mahnung", „Ihre Rechnung" oder „Inkasso" in der Betreffzeile misstrauisch, oftmals verbergen sich dahinter Gaunereien.
- Seien Sie ebenso vorsichtig bei Gewinnbenachrichtigungen und Angeboten zum Geldtransfer, oft verraten sich unseriöse Nachrichten mit einem Betreff, der den Adressaten neugierig machen soll.

2.8 Download mit Maß

- Laden Sie Programme oder Dateien nur von Ihnen bekannten und vertrauenswürdigen Seiten auf Ihren Rechner.
- Vertrauen Sie im Zweifel auf Originalsoftware, denn Gratis-Angebote dubioser Anbieter könnten mit Schadprogrammen infiziert sein.
- Achten Sie bei vermeintlich kostenlosen Diensten auf das „Kleingedruckte", ein Download kann unter Umständen in einem kostenpflichtigen Vertrag münden (Abo-Falle).
- Widersprechen Sie unberechtigten Zahlungsaufforderungen und holen Sie sich professionellen Rat.
- Seien Sie besonders aufmerksam, wenn Sie vor dem Download zur Eingabe Ihrer persönlichen Daten aufgefordert werden, dies kann ein Hinweis auf eine Falle sein.

- Prüfen Sie vor dem Download per Suchmaschine die Seriösität des Anbieters.
- Achten Sie bei dem Herunterladen von Musik, Filmen oder Spielen, insbesondere im Rahmen von Tauschbörsen darauf, dass keine Urheberrechte verletzt werden.

2.9 Abzockern keine Chance

- Lesen Sie das Kleingedruckte genau. Vermeintlich kostenlose Dienste entpuppen sich beim Lesen der Allgemeinen Geschäftsbedingungen oft als kostenpflichtig. Achten Sie auf versteckte Kostenhinweise.
- Klicken Sie sich nicht unbedarft durch Anmeldeformulare. Durch ein gesetztes oder fehlendes Häkchen könnten sie ungewollt den Verzicht auf Ihr Widerrufsrecht erklären.
- Lassen Sie sich nicht mit Sach- oder Geldpreisen zur Eingabe Ihrer persönlichen Daten ködern.
- Prüfen Sie die Angaben im Impressum. Unseriöse Anbieter hinterlegen oft nur die Adresse eines Postfaches, Auslandsadressen oder schalten Telefonnummern mit Bandansagen.
- Lassen Sie sich nicht von Internetadressen irreführen, die denen bekannter Anbieter täuschend ähnlich sind.

2.10 Hilfe nutzen

- Fragen Sie Bekannte oder Verwandte nach Ihren Erfahrungen mit dem Internet und lassen Sie sich bei den ersten Schritten begleiten.
- Nehmen Sie bei Bedarf Beratung und Hilfe Ihrer örtlichen Verbraucherzentrale in Anspruch.
- Erstatten Sie Anzeige bei der Polizei, wenn Sie trotz aller Vorsicht Opfer einer Straftat geworden sind.
- Nutzen Sie einschlägige Fortbildungsangebote Ihrer regionalen Bildungsträger (z. B.: Volkshochschule).

Informieren Sie sich unter anderem weiter auf folgenden Internetseiten:

www.bsi-fuer-buerger.de

www.polizei-beratung.de

www.verbaucherzentrale.de

www.internet-sicherheit.de

www.internet-guetesiegel.de

www.trustedshops.de

www.safer-shopping.de

www.computerbetrug.de

www.verbraucher-sicher-online.de

Herausgeber:
Landesrat für Kriminalitätsvorbeugung Mecklenburg-Vorpommern (LfK), Geschäftsstelle,
Innenministerium Mecklenburg-Vorpommern, Alexandrinenstr. 1, 19055 Schwerin
Telefon: (03 85) 5 88 - 24 60, lfk@kriminalpraevention-mv.de, www.kriminalpraevention-mv.de

Bildnachweis: Titel: © Yuri Arcurs-Fotolia.com, Seite 2: © Alterfalter-Fotolia.com, Seite 8: © Marzanna Syncerz-Fotolia.com