Zeitschrift: Visit : Magazin der Pro Senectute Kanton Zürich

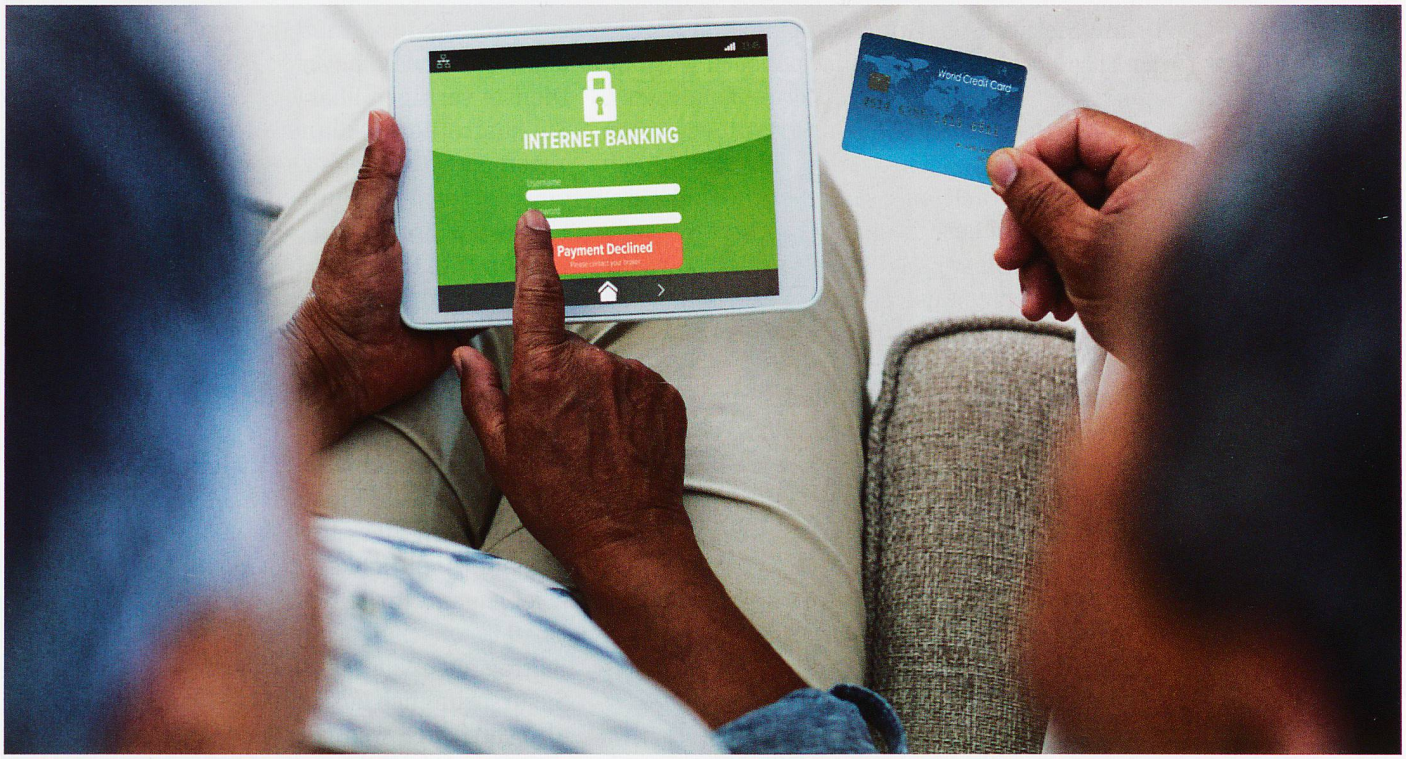
Band: - (2019)

Heft: 3: Älter werden in einer digitalen Welt : die Chancen und Risiken der Online-Technologie

Artikel: So schützen Sie sich im Internet

Autor: Fargahi, Nina

DOI: https://doi.org/10.5169/seals-928407



Auch im Internet und in den sozialen Netzwerken sollten zur eigenen Sicherheit ein paar wichtige Punkte beachtet werden.

So schützen Sie sich im Internet

Die digitale Welt kann verführen und helfen. Sie kann aber auch Gefahren bergen. Die wichtigsten Tipps zum Umgang mit digitalen Medien.

Text: **Nina Fargahi**

Viele denken, dass Social Media noch ausschliesslich das Reich der jüngeren Generationen seien. Doch auch viele ältere Menschen sind mittlerweile auf den Geschmack gekommen. Sie nutzen das Internet und die sozialen Netzwerke mit viel Enthusiasmus. Viele Grosseltern kennen sich bestens aus mit Skype oder Facebook, chatten mit Angehörigen oder nehmen Kontakt auf mit längst aus den Augen verlorenen Freunden aus früheren Zeiten.

Doch auch hier ist Vorsicht die Mutter der Porzellankiste. Deshalb sollten auch im Internet und in den sozialen Netzwerken ein paar wichtige Punkte beachtet werden:

Verwenden Sie lange Passwörter. Sie sollten mindestens acht Zeichen sowie Zahlen, Symbole und Gross- und Kleinbuchstaben enthalten. Vermeiden Sie die Verwendung von Namen oder Geburtstagen. Gute Passwörter bestehen aus kurzen Sätzen, die Sie sich merken können. Beispiel: «Dieses P@ssw0rt vergesse 1ch nie!!»

Geben Sie Ihre persönlichen Passwörter niemals an Dritte weiter. Es sei denn, Sie haben jemanden bestimmt, dem Sie für die Verwaltung Ihrer Konten vertrauen. Somit verhindern Sie, dass sich jemand in Ihr Konto einloggt und es für missbräuchliche Zwecke benutzt. >>

Foto: Adobe Stock

Teilen Sie keine heiklen Informationen. Senden Sie niemandem heikle Informationen wie Kontonummern oder Sozialversicherungsnummern. Viele Betrüger geben sich auch als Unternehmen aus, um Informationen von Senioren zu erhalten – genau wie am Telefon. Es gilt: Seriöse Unternehmen mit einem berechtigten Bedarf an Informationen wissen, dass E-Mails und soziale Netzwerke für den Datenaustausch nicht sicher sind, und wenden andere Methoden an.

Posten Sie nicht auf Social Media, dass Sie unterwegs sind. Viele Kriminelle nutzen soziale Netzwerke und konzentrieren sich auf die Häuser derjenigen, die öffentlich machen, wann und wo sie unterwegs sind.

Aktivieren Sie die Datenschutzeinstellungen. Es lohnt sich, die Datenschutzrichtlinien und die entsprechenden Einstellungen eines Dienstes kennenzulernen, bevor sie ihn nutzen. Fast alle Dienste verfügen über Einstellungen, mit denen Sie kontrollieren können, wer Ihre Publikation sehen darf. Facebook zum Beispiel verfügt über eine Reihe von Steuerelementen, mit denen nur bestimmte Freunde Ihre Posts sehen können. Sie können Ihre Beiträge auch beschränken auf eine Gruppe, zum Beispiel nur auf Familienmitglieder. Es gibt auch Einstellungen für Smartphones, die einschränken, wer Zugriff auf Ihren Standort, Kontakte und andere persönliche Daten hat.

Seien Sie sich der Öffentlichkeit bewusst. Auch wenn Sie private Einstellungen aktiviert haben, kann es sein, dass Ihre Texte und Bilder in die breitere Öffentlichkeit gelangen. Wenn zum Beispiel jemand Ihren Beitrag teilt und gleichzeitig keine Datenschutzbestimmungen nutzt, kann Ihr Beitrag auch von Menschen gelesen werden, die Sie ursprünglich ausschliessen wollten. Seien Sie also vorsichtig, wenn Sie andere Menschen in Geschichten oder Bildern kennzeichnen. Bedenken Sie, dass auch Arbeitgeber, Versicherungsgesellschaften oder Firmen Ihren Post sehen können.

Melden Sie Missbrauch. Wenn Sie Nachrichten in den Social Media oder in Ihrem Mail-Konto erhalten, die Ihnen verdächtig oder missbräuchlich erscheinen, öffnen Sie auf keinen Fall angefügte Dateien und antworten Sie nicht. Melden Sie es einer Person, der Sie vertrauen, oder dem entsprechenden Dienst. Fast alle Websites sowie Online- und Mobilfunkanbieter haben Mitarbeiter, die auf Beschwerden reagieren. Meldungen nimmt auch MELANI entgegen, die Melde- und Analysestelle Informationssicherung des Bundes; hier finden Sie auch weitere Informationen, wie Sie sich vor Gefahren im Internet schützen können.

Nützliche Infos zur Sicherheit im Internet:
www.melani.admin.ch | www.connectsafely.org (in Englisch)

Digitale Friedhöfe

Wenn ein Mensch stirbt, gibt es viel zu regeln – immer häufiger auch beim digitalen Nachlass. Dabei ist oft gar nicht bekannt, wo der Verstorbene überall online angemeldet war. Und selbst wenn man es weiss, sind die Zugänge normalerweise gesichert durch Passwörter. Es kann auch sein, dass kostenpflichtige Abonnements weiterlaufen. Um alles zu kündigen, sind die Sterbeurkunde und der Erbschein hilfreich. Dann gewähren die meisten Anbieter den Angehörigen Zugang zu den Daten im Internet. Hilfreich ist es, noch zu Lebzeiten eine Liste anzulegen, in der Benutzernamen und Passwörter der Online-Zugänge aufgelistet sind. Allerdings sollte man die Liste nicht neben dem Computer aufbewahren. Es gibt sogenannte Passwort-Manager, die auf einem USB-Stick die Passwörter verschlüsselt speichern und Änderungen automatisch abgleichen können. Dieser Stick ist dann ebenfalls mit einem hoffentlich guten Passwort geschützt, das man dem Testament beifügen kann.
Auch in diesem Fall gilt: Wenn man rechtzeitig Vorkehrungen trifft, macht man es seinen Angehörigen leichter.