Passwort-Gruppen bilden. Dabei verwenden Sie dasselbe Passwort für eine bestimmte Gruppe von Benutzerkonten, z. B.: unwichtige Accounts, wichtige Accounts, Spiele-Websites, E-Mail-Konten etc.
- Alternativ dazu können Sie einen Passwort-Safe bzw. einen Passwort-Manager verwenden

11

Was ist ein Passwort-Manager?

Hier werden viele verschiedene Passwörter hinter einem Master-Passwort abgespeichert. Der Vorteil: Sie brauchen sich nur ein Passwort merken. Bekannte Passwort-Manager sind zum Beispiel LastPass, 1Password, Keeper und KeePass.

12

Was ist beim Aufschreiben von Passwörtern wichtig?

- Bezeichnen Sie ein Passwort nie als Passwort
- Notieren Sie keine ergänzenden Zugangsdaten zum Passwort
- Bewahren Sie Passwörter nie direkt am Computer oder Handy auf
- Verschlüsseln Sie Ihr Passwort zusätzlich, z. B. durch Buchstaben-, Silben- oder Zahlendreher – schreiben Sie also statt „29“ „92“

Ändern Sie Ihr Passwort sofort, wenn Ihr Service-Anbieter gehackt wurde oder wenn Sie glauben, dass eine unbefugte Person Ihr Passwort herausgefunden hat.

13

Was ist Phishing?

Das Wort „Phishing“ leitet sich von „password fishing“ ab. Damit werden verschiedene Tricks bezeichnet, die alle ein Ziel haben: Ahnungslosen Internetnutzerinnen bzw. –nutzern geheime Daten zu entlocken – z. B. Daten für das Online-Banking, für Kleinanzeigen-Plattformen, Online-Shops oder Soziale Plattformen.

14

Wie läuft Phishing ab?

In der Regel werden betrügerische E-Mails, Chatnachrichten oder SMS versendet. Dabei werden Sie aufgefordert, Links oder Dateianhänge zu öffnen und anschließend persönliche Daten bekanntzugeben oder Apps herunterzuladen.

ACH TUNG

Lassen Sie sich nicht in die Irre führen – weder von vertraut aussehenden Firmenlogos noch von täuschend echt aussehenden Links.

In Wahrheit handelt es sich um gefälschte Websites.
Die Betrügerinnen bzw. Betrüger hoffen, dass Sie dort Ihre Zugangsdaten eingeben oder Apps herunterladen. Damit können sie dann auf Ihre Kosten illegale Zahlungen veranlassen oder im Internet einkaufen.

Oft werden Pishing-Mails auch von gefährlichen E-Mail-Anhängen begleitet. Nach dem Öffnen installiert sich Schadsoftware, die dann unbemerkt Passwörter und andere vertrauliche Daten auf Ihrem Computer, Tablet oder Smartphone ausspioniert.

Unternehmen und Banken verlangen **niemals** vertrauliche Daten wie Logins, Passwörter oder Transaktionsnummern per E-Mail oder Chat von Ihnen.

15

Wie schützen Sie sich vor Phishing?

- **Links in E-Mails**
  Klicken Sie in E-Mails oder sonstigen Nachrichten auf keine Links mit der Aufforderung, Ihre Kontodaten oder Passwörter bekannt zu geben. Auch nicht, um nähere Informationen zu erhalten. Löschen Sie diese E-Mails!

- **Login-Daten, Passwörter, TANs**
  Übermitteln Sie keine vertraulichen Daten per E-Mail, per Chat oder telefonisch. Nutzen Sie Zwei-Faktor-Authentifizierungen (Frage 9).

- **Datei-Anhänge**
  Öffnen Sie keinesfalls unbekannte Datei-Anhänge in E-Mails oder sonstigen Nachrichten. Darin sind oft Viren etc. versteckt.

- **Änderungen auf der vertrauten Login-Seite**
  Melden Sie überraschende Änderungen auf einer Ihnen vertrauten Login-Seite sofort an den Betreiber, also z. B. an Ihre Bank.

- **SSL-verschlüsselte Seiten**
  Geben Sie vertrauliche und persönliche Daten ausschließlich über SSL-verschlüsselte Seiten bekannt. Diese Seiten erkennen Sie am „https://“ am Beginn der Internetadresse und an einem versperrten Schloss-Symbol am oberen oder unteren Bildschirmrand.

- **Sicherheits-Updates und Anti-Viren-Programme**
  Führen Sie laufend Sicherheits-Updates durch und installieren Sie ein Anti-Viren-Programm und eine Firewall.

Wichtig

Selbstverständlich erarbeiten wir alle Inhalte unserer Ratgeber sorgfältig. Dennoch können wir nicht garantieren, dass alles vollständig und aktuell ist bzw. sich seit dem Druck keine Gesetzesänderung ergeben hat. Bei individuellen Fragen steht Ihnen unsere Hotline zur Verfügung: (01) 501 65 0

Weitere Informationen finden Sie auch im Internet:
www.arbeiterkammer.at

Alle aktuellen AK Publikationen stehen zum Download für Sie bereit: wien.arbeiterkammer.at/publikationen

Weitere Bestellmöglichkeiten:
- E-Mail: bestellservice@akwien.at
- Bestelltelefon: (01) 501 65 1401

Artikelnummer 430
1. Druckauflage, Oktober 2018

Impressum
Medieninhaber: Kammer für Arbeiter und Angestellte für Wien,
Prinz-Eugen-Str. 20-22, 1040 Wien, Telefon (01) 501 65 0
Offenlegung gem. § 25 MedienG: siehe wien.arbeiterkammer.at/impressum
Zulassungsnummer: MZ 02Z34648 M
Inhalt: In Kooperation mit saferinternet.at
Titelfoto: gpointstudio - Adobe Stock
Grafik: www.typofactory.at
Druck: Ferdinand Berger & Söhne GmbH, 3580 Horn
Verlags- und Herstellungsort: Wien

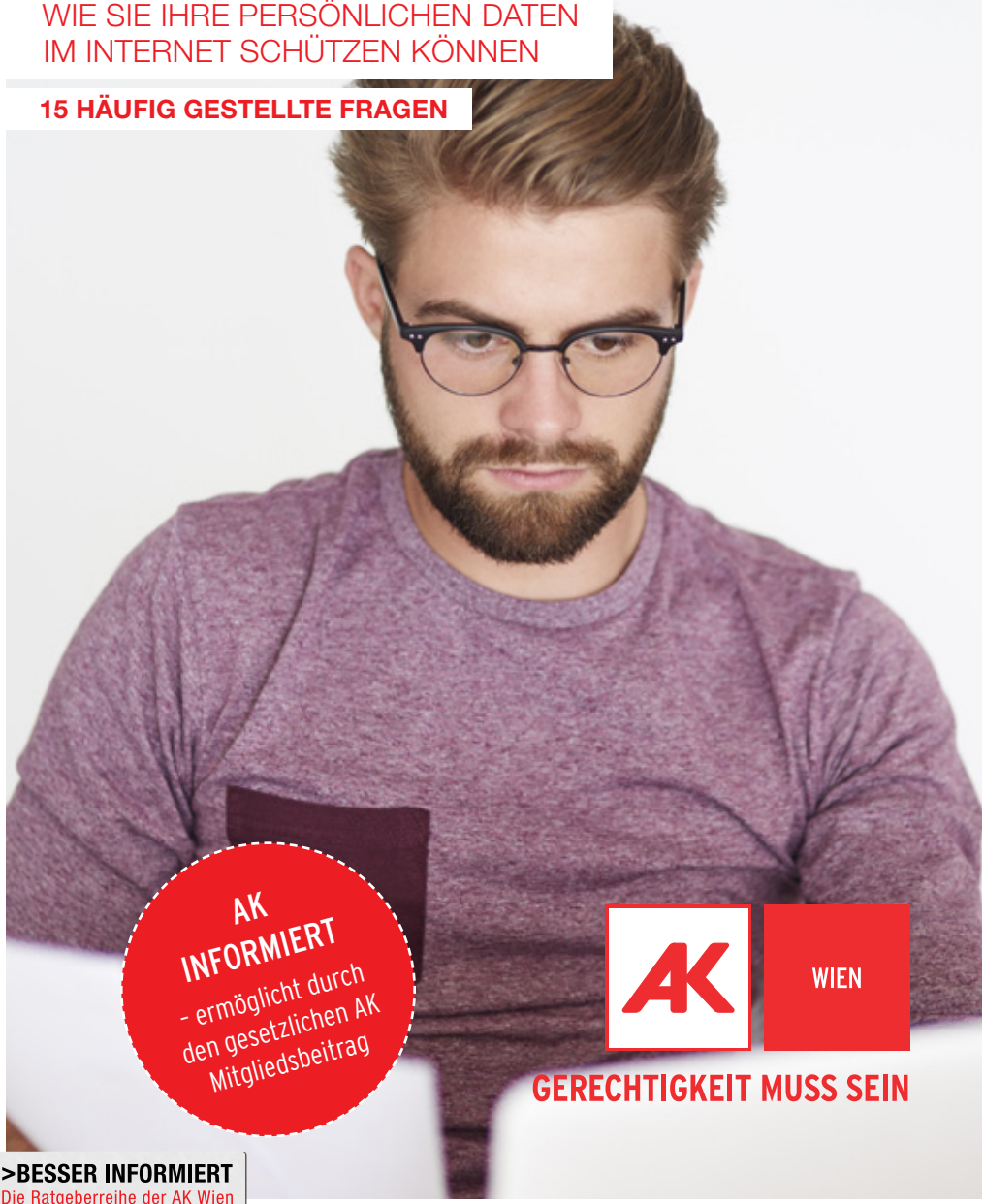
Stand: Oktober 2018

Saferinternet.at
Das Internet sicher nutzen!

DATENKLAU

WIE SIE IHRE PERSÖNLICHEN DATEN
IM INTERNET SCHÜTZEN KÖNNEN

15 HÄUFIG GESTELLTE FRAGEN



AK INFORMIERT
- ermöglicht durch den gesetzlichen AK Mitgliedsbeitrag

AK WIEN

GERECHTIGKEIT MUSS SEIN

>BESSER INFORMIERT
Die Ratgeberreihe der AK Wien

Warum ist Datenschutz im Internet wichtig?

Das Internet vergisst nicht. Einmal veröffentlichte Daten sind weltweit zugänglich und oft nicht mehr zu entfernen. Zudem ist das Internet ein Paradies für Datensammler. Immer wieder ermöglichen Sicherheitslücken den unerlaubten Zugriff auf Nutzerdaten.

Deshalb: Sichern Sie Ihre persönlichen Daten! Wie das geht, erfahren Sie in diesem Folder anhand häufig gestellter Fragen.

1

Was gilt grundsätzlich?

Die wichtigste Regel
Veröffentlichen Sie so wenig personenbezogene Daten wie möglich! Adresse, Telefonnummer, Passwörter etc. gehen Fremde nichts an. Seien Sie besonders sparsam mit diesen Informationen, wenn Sie sich auf Websites, für Gewinnspiele und dergleichen registrieren.

TIPP

Wann immer es möglich ist: Verwenden Sie anonyme Nicknames anstelle Ihres richtigen Namens.

2

Welche E-Mail-Adresse verwenden Sie?

Verwenden Sie mehrere E-Mail-Adressen. Legen Sie sich bei einem Gratis-Anbieter eine zusätzliche E-Mail-Adresse an, die keine Rückschlüsse auf Ihre Person zulässt – z. B. bei Yahoo!, Hotmail oder Gmail. Verwenden Sie diese Adresse, wenn Sie sich auf Websites registrieren, in Blogs posten oder in Foren diskutieren.

3

Wie reagieren Sie auf Spam?

Ignorieren Sie Spam und antworten Sie niemals auf Spam-E-Mails. Damit bestätigen Sie nur, dass Ihre E-Mail-Adresse gültig ist. Dadurch bekommen Sie in Folge noch mehr Spam-Nachrichten.

ACHTUNG

Öffnen Sie auch keine unbekannten Dateianhänge aus E-Mails. Es könnte sich um Spyware handeln, die persönliche Daten auf Ihrem Computer ausspioniert oder Viren enthält.

4

Wie gehen Sie online am besten vor?

Hinterfragen Sie Ihr Online-Verhalten
Was enthält Ihre Website, Ihr Blog oder Ihr Community-Profil? Auch Fotos oder Angaben, die Sie eigentlich nicht öffentlich machen wollen? Bedenken Sie immer: Alle Inhalte sind weltweit frei zugänglich und über Suchmaschinen leicht zu finden.

Schränken Sie Ihr Community-Profil ein. Nutzen Sie die Privatsphäre-Einstellungen in Sozialen Netzwerken. Und achten Sie darauf, dass nur ausgewählte Personen Ihre persönliche Daten einsehen können..

5

Können Sie Ihren Computer sicherer machen?

Ja. Optimieren Sie die Sicherheitseinstellungen Ihres Browsers:

- **Mozilla Firefox:** Extras – Einstellungen – Sicherheit bzw. Datenschutz
- **Internet Explorer:** Extras – Internetoptionen – Sicherheit bzw. Datenschutz

Weitere wichtige Schutzmaßnahmen:

- Führen Sie regelmäßig Updates durch
- Verwenden Sie ein Anti-Viren-Programm und eine Firewall
- Verschlüsseln Sie Ihre WLAN-Verbindung

6

Worauf sollten Sie bei der Nutzung öffentlicher Computer achten?

Seien Sie besonders vorsichtig bei der Nutzung öffentlicher Computer, zum Beispiel in Schulen, Bibliotheken oder Internet-Cafés. Allzu sensible Daten – wie z. B. Bankdaten – sollten Sie hier am besten gar nicht eingeben. Wenn Sie sich auf Websites einloggen, melden Sie sich auch stets wieder ab. Nutzen Sie verschlüsselte Seiten.

7

Wie sieht ein sicheres Passwort aus?

Grundsätzlich gilt: Hundertprozentigen Schutz gibt es nicht. Auch ein langes, kompliziertes Passwort kann geknackt werden. Doch Sie können es möglichen Angreifern schwerer machen, indem Sie Ihre Passwörter möglichst sicher gestalten:

- Je länger ein Passwort ist, desto sicherer ist es. Diese Regel gilt ab mindestens 12 Zeichen. Siehe auch „4-Wörter-Methode“
- Verwenden Sie keine leicht zu erratenden Informationen wie Ihr Geburtsdatum oder den Namen eines Familienmitgliedes
- Verwenden Sie für jeden Login ein eigenes Passwort
- Nutzen Sie Passwort-Manager, z. B. Keepass, LastPass,1Password

8

Welche Strategien gibt es?

- **4-Wörter-Methode**
  Mit dieser Strategie können Sie ganz leicht lange, zufällige und dadurch komplexe Passwörter erstellen.
  Z. B.: FahrradTopfenSieglindeMeeresgrund

- **Zeichen schlagen Wörter**
  Reichern Sie Ihr Passwort mit Sonderzeichen und Zahlen an. Z. B.: Fahrrad&Topfen3Sieglinde%Meeresgrund9!

- **Minimum 12 Zeichen**
  Ihr Dienst hat gänzlich andere Vorgaben? Dann verwenden Sie ein Passwort mit mindestens 12 Zeichen. Variieren Sie Groß- und Kleinschreibung und kombinieren Sie Buchstaben, Zahlen und Sonderzeichen wie + = ? & $ % „ ( ) / * >< .

9

Was bedeutet Zwei-Faktor-Authentifizierung?

Die Zwei-Faktor-Authentifizierung – auch Zwei-Schritte- oder Zwei-Wege-Authentifizierung – ist eine zusätzliche Sicherheits-Maßnahme zum Schutz von Benutzerkonten. Hier geben Sie zusätzlich zum Passwort beim Login z. B. einen PIN-Code ein. Dieser Code wird etwa auf Ihre im Konto hinterlegte Handynummer gesendet oder es wird ein Code-Generator eingesetzt. Der Vorteil: Selbst, wenn Ihr Passwort in falsche Hände gelangt, haben Unbefugte keinen Zugriff auf Ihr Benutzerkonto.

TIPP Auf twofactorauth.org finden Sie eine Liste an Online-Diensten, die eine Zwei-Faktor-Authentifizierung anbieten.

TIPP Finden Sie heraus, ob Ihre Identität – E-Mail-Adresse, Passwörter etc. – bereits einmal Opfer eines Datenklaus wurden: haveibeenpwned.com oder sec.hpi.de/ilc/search

10

Wie können Sie Passwörter sicher aufbewahren?

- Halten Sie Ihre Passwörter geheim
- Geben Sie Passwörter stets unbeobachtet von Dritten ein
- Speichern Sie Passwörter nie im Browser ab – das ist jenes Programm, mit dem Sie Internetseiten abrufen können. Vor allem dann nicht, wenn der Computer bzw. das Smartphone oder Tablet von mehreren Personen verwendet wird
- Verwenden Sie unterschiedliche Passwörter für unterschiedliche Benutzerkonten. Das ist Ihnen zu mühsam? Dann können Sie auch