CL-05 | CHECKLISTE · 22.07.2026 · V.1.0.0

IT-Sicherheit im Alltag

Die Jahres-Checkliste von 1.wien für Privathaushalte, Einzelunternehmen und kleine Betriebe.

Die meisten Vorfälle, die bei uns landen, brauchen keinen hochgerüsteten Angreifer. Sie brauchen ein wiederverwendetes Passwort, ein aufgeschobenes Update oder einen Klick auf eine täuschend echte Rechnung. Genau dort setzt diese Liste an.

> **Wenn Sie nur drei Dinge umsetzen**
> **Erstens:** ein eigenes, langes Passwort für Ihr E-Mail-Konto – es ist der Generalschlüssel zu allen anderen Konten. **Zweitens:** Zwei-Faktor-Anmeldung überall dort, wo Geld oder Identität hängen. **Drittens:** ein Backup, das offline liegt.

01 Passwörter und Anmeldung

- [ ] Für jeden Dienst ein eigenes Passwort
  Ein einziges wiederverwendetes Passwort reicht, damit aus einem fremden Datenleck Ihr Problem wird.
- [ ] Passwort-Manager im Einsatz
  Der einzige praktikable Weg zu vielen guten Passwörtern. Ein starkes Hauptpasswort, den Rest übernimmt das Programm.
- [ ] Lange Passphrasen statt kurzer Sonderzeichen-Kombinationen
  Vier zufällige Wörter sind sicherer und leichter zu merken als „Xk7!q“.
- [ ] Zwei-Faktor-Anmeldung aktiviert
  E-Mail, Bank, Microsoft- bzw. Apple-Konto, Steuerportal, soziale Netzwerke, Onlineshops mit hinterlegter Zahlung.
- [ ] App oder Sicherheitsschlüssel statt SMS-Code verwenden, wo möglich
- [ ] Wiederherstellungscodes ausgedruckt und sicher verwahrt
- [ ] E-Mail-Adressen auf bekannte Datenlecks geprüft
- [ ] Passwörter nicht im Browser ohne Hauptpasswort speichern
- [ ] Bildschirmsperre mit kurzer Zeitspanne aktiviert

02 Updates und Schadsoftware

- [ ] Automatische Updates für Betriebssystem aktiviert
- [ ] Browser, Office und PDF-Reader aktuell
- [ ] Virenschutz aktiv und aktuell
  Der eingebaute Schutz von Windows genügt für die meisten Privatanwender – wichtig ist, dass er wirklich aktiv ist.
- [ ] Keine Software aus Suchmaschinen-Anzeigen installieren
  Gefälschte Downloadseiten für bekannte Programme sind eine der häufigsten Infektionsquellen.
- [ ] Nicht mehr unterstützte Betriebssysteme abgelöst
- [ ] Administratorrechte nur bei Bedarf verwenden
  Ein Standardkonto für die tägliche Arbeit begrenzt den Schaden erheblich.
- [ ] Makros in Office-Dokumenten aus dem Internet blockiert

03 Phishing und Betrugsmaschen erkennen

Angreifer kopieren heute Layout, Logo und Tonfall fehlerfrei. Achten Sie auf die Absicht, nicht auf die Rechtschreibung.

- [ ] Zeitdruck und Drohungen als Warnsignal werten
  „Ihr Konto wird in 24 Stunden gesperrt" ist eine Methode, kein Anliegen.
- [ ] Links vor dem Klick prüfen: Was steht direkt vor dem ersten Schrägstrich nach https://?
- [ ] Bei Zahlungsaufforderungen einen zweiten Kanal nutzen
  Beim bekannten Ansprechpartner unter der gespeicherten Nummer anrufen – nicht unter der Nummer aus der E-Mail.
- [ ] Geänderte Bankverbindungen in Rechnungen immer telefonisch bestätigen
  Der klassische Rechnungsbetrug bei Kleinbetrieben.
- [ ] Keine Fernwartungssoftware auf Zuruf am Telefon installieren
  Weder Microsoft noch Ihre Bank noch die Polizei rufen unaufgefordert an.
- [ ] Anhänge nur öffnen, wenn Absender und Anlass erwartet wurden
- [ ] QR-Codes auf Aufklebern und Briefen misstrauisch behandeln
- [ ] Team informiert: Alle wissen, an wen sie Verdachtsfälle melden

04 Netzwerk und Router

- [ ] Standard-Passwort der Router-Oberfläche geändert
- [ ] WLAN mit WPA2 oder WPA3 und langem Passwort abgesichert
- [ ] WPS deaktiviert
- [ ] Fernzugriff auf den Router aus dem Internet abgeschaltet
  Ebenso UPnP, sofern nicht ausdrücklich benötigt.
- [ ] Router-Firmware aktuell
- [ ] Gäste-WLAN für Besuch und Smart-Home-Geräte eingerichtet
  Trennt Kameras, Fernseher und Steckdosen von Ihren Arbeitsgeräten.
- [ ] Portweiterleitungen durchgesehen und Unnötiges entfernt
- [ ] Netzwerkfreigaben geprüft: Wer sieht welche Ordner?
- [ ] Smart-Home- und IoT-Geräte inventarisiert und aktualisiert

05 Geräte, Verschlüsselung und unterwegs

- [ ] Festplattenverschlüsselung aktiv
  BitLocker unter Windows, FileVault bei Apple. Wiederherstellungsschlüssel getrennt vom Gerät aufbewahren.
- [ ] Handy und Tablet mit Code, nicht nur mit Wischmuster gesichert
- [ ] Gerät-suchen-Funktion und Fernlöschung eingerichtet
- [ ] Automatische Sperre bei Inaktivität aktiviert
- [ ] In öffentlichen Netzen VPN verwenden oder auf mobile Daten wechseln
  Hotel, Café, Flughafen, Bahn.
- [ ] Keine fremden USB-Sticks anschließen
- [ ] Sichtschutzfolie bei Arbeit in der Öffentlichkeit erwägen
- [ ] Altgeräte vor Weitergabe sicher löschen, nicht nur zurücksetzen

06 Konten, Rollen und Datenschutz

Besonders für Betriebe, Vereine und Ordinationen.

- [ ] Übersicht aller Konten und Zugänge dokumentiert
- [ ] Zugriffe ausgeschiedener Mitarbeitender entzogen
  Auch bei Cloud-Diensten, Kassensystem und gemeinsamen Postfächern.
- [ ] Rollen nach dem Prinzip der geringsten Rechte vergeben
- [ ] Geteilte Sammelkonten aufgelöst
- [ ] Verzeichnis der Verarbeitungstätigkeiten aktuell (DSGVO)
- [ ] Auftragsverarbeitungsverträge mit Dienstleistern vorhanden
  Hosting, Cloud-Speicher, Steuerberatung, IT-Betreuung.
- [ ] Verantwortliche Person für Meldungen nach DSGVO benannt
  Ein meldepflichtiger Vorfall muss binnen 72 Stunden gemeldet werden.
- [ ] Mitarbeitende einmal jährlich geschult

07 Wenn es passiert ist

Die ersten dreißig Minuten entscheiden über das Ausmaß.

- [ ] Betroffenes Gerät vom Netz trennen, aber eingeschaltet lassen, bis Hilfe da ist.
  Bei Servern geordnet herunterfahren – nicht den Stecker ziehen.
- [ ] Backup-Medien sofort physisch trennen.
- [ ] Passwörter von einem sauberen Gerät aus ändern – E-Mail zuerst.
- [ ] Bank verständigen und Zahlungen sperren lassen, wenn Zahlungsdaten betroffen sind.
- [ ] Alles dokumentieren: Zeitpunkt, Fehlermeldungen, betroffene Geräte.
  Fotos genügen. Diese Notizen brauchen Versicherung und Behörde.
- [ ] Kein Lösegeld zahlen und nicht mit Erpressern verhandeln.
- [ ] Fachliche Hilfe holen.

Stelle	Zuständig für	Kontakt
1.wien e.U.	Erstbewertung, Bereinigung, Wiederherstellung	+43 660 815 04 12 · 1@1.wien
Cyber-Security-Hotline der Wirtschaftskammern	Kostenlose Erstinformation für Mitgliedsbetriebe, rund um die Uhr	0800 888 133
Cybercrime Helpline der Stadt Wien	Erstberatung für Wienerinnen und Wiener, werktags 7:30–17:00	01 4000-4006
Meldestelle für Internetkriminalität (Bundeskriminalamt)	Meldung bei Verdacht auf Internetkriminalität	against-cybercrime@bmi.gv.at
Nächste Polizeidienststelle	Strafanzeige bei konkretem Schaden	persönlich vor Ort
Österreichische Datenschutzbehörde	Meldung von Datenschutzverletzungen binnen 72 Stunden	dsb.gv.at
Watchlist Internet	Aktuelle Betrugsmaschen nachschlagen	watchlist-internet.at

Angaben ohne Gewähr

Rufnummern und Zuständigkeiten können sich ändern. Prüfen Sie im Ernstfall die aktuellen Angaben auf onlinesicherheit.gv.at oder rufen Sie uns an – wir übernehmen die Koordination.

NOTIZEN / OFFENE PUNKTE

Sicherheits-Check durch 1.wien

Wir gehen diese Liste gemeinsam mit Ihnen durch, prüfen Router, Konten und Backups und übergeben einen schriftlichen Befund mit priorisierten Maßnahmen. · Siegfriedgasse 23, 1210 Wien · +43 660 815 04 12 · 1@1.wien · 1.wien