6/25

# PRIVACY@WORK

## DATENSCHUTZ FÜR MITARBEITER


PASSKEY

**Die sichere und einfache Passwort-Alternative im Jahr 2025**

ARBEITSMITTEL TEILEN

**Nicht Ihr Gerät? Datenschutz beim Teilen von Arbeitsmitteln**

powered by
PRIVACYXPERTS

*Liebe Leserin, lieber Leser,*

*es sind oft die kleinen Dinge, die den Unterschied machen – ein vergessener Klick, ein geteilter Zugang, ein schnell weitergereichtes Gerät. In unserem digitalen Alltag arbeiten wir effizient, vernetzt und flexibel – aber manchmal auch ein bisschen zu sorglos. Genau hier setzen unsere Themen in dieser Ausgabe an.*

***Passkeys** versprechen eine neue Ära der digitalen Sicherheit: keine Passwörter mehr, keine Zettel unter der Tastatur, keine mühsamen Merkhilfen – dafür ein modernes Verfahren, das Komfort mit Schutz verbindet. Doch wie funktioniert das genau? Und was muss man beachten, damit aus der cleveren Technik auch tatsächlich mehr Sicherheit wird? Wir erklären es Ihnen verständlich und praxisnah.*

*Gleichzeitig werfen wir einen Blick auf einen anderen Aspekt der IT-Sicherheit, der im Alltag oft übersehen wird: das **Teilen von Arbeitsmitteln.** Ob Laptop, Headset oder Zugangsdaten – viele von uns greifen gelegentlich auf fremde Geräte oder Accounts zurück. Praktisch? Ja. Aber auch riskant. Denn wenn der eigene Benutzername unter einer fremden E-Mail steht oder ein USB-Stick plötzlich das Firmennetzwerk lahmlegt, wird aus „nur mal kurz" schnell ein echtes Problem.*

*Diese Ausgabe lädt Sie ein, genauer hinzusehen – auf Technik, auf Gewohnheiten, auf die kleinen Momente, in denen Datenschutz und IT-Sicherheit beginnen.*

*Mit freundlichen Grüßen*

*Ihr Redaktionsteam von „Privacy@Work"*

**SEBASTIAN TAUSCH**
ARBEITET ALS SELBSTSTÄNDIGER IT-BERATER UND UNTERSTÜTZT KLEINE UND MITTLERE UNTERNEHMEN PRAXISNAH IM BEREICH DATENSCHUTZ. NACH EINER KAUFMÄNNISCHEN AUSBILDUNG SAMMELTE ER VIELE JAHRE PRAKTISCHE IT-ERFAHRUNG.

**ANDREAS HESSEL**
IST ALS CHIEF INFORMATION SECURITY OFFICER LANGJÄHRIGER LEITER DES BEREICHES INFORMATIONSSICHERHEIT UND RISIKOMANAGEMENT EINER LANDESBANK. DANEBEN ARBEITET ER ALS EXTERNER DATENSCHUTZBEAUFTRAGTER UND BERATER IM BEREICH CYBERSECURITY.

# PASSKEY – DIE SICHERE UND EINFACHE PASSWORT-ALTERNATIVE IM JAHR 2025

**Die meisten von uns nutzen täglich eine Vielzahl an Onlinediensten – vom E-Mail-Postfach bis zum kompletten Onlineoffice und Onlineanwendungen. Damit steigt auch die Zahl der Passwörter, die wir verwalten müssen. Und genau hier setzen sogenannte Passkeys an. Sie können Passwörter nicht nur ersetzen, sondern auch viele Risiken im Zusammenhang mit Datendiebstahl und Phishing reduzieren. Was genau dahintersteckt und was Sie beachten sollten, erfahren Sie in diesem Beitrag. Eine weitere gute Nachricht zu Beginn ist sicherlich, dass die Verarbeitung im Hintergrund kompliziert ist – aber nicht für uns Anwender in der täglichen Nutzung.**

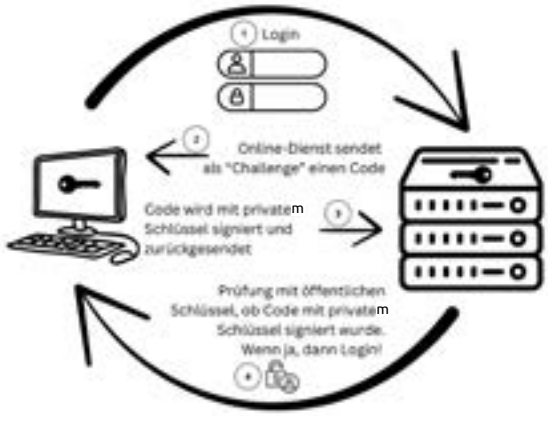
## So erfolgt die Anmeldung mit Passkey

Die Anmeldung mit Passkey ist auf den ersten Blick ähnlich wie die klassische Anmeldung mit Benutzername und Passwort. Nur gibt der Benutzer kein Passwort auf der Anmeldeseite ein. Stattdessen tippen manche Benutzer einen Code auf der Tastatur ein, andere schauen in die Kamera oder scannen mit dem Smartphone ihren Fingerabdruck. Allerdings ist diese Eingabe, etwa die PIN, kein Ersatz für das Passwort – auch wenn es so erscheint!

### Was sind Passkeys?

Die PIN, Fingerabdruck oder Gesichtserkennung bei der Passkey-Anmeldung schützen den privaten digitalen Schlüssel, der für diese Anmeldeseite erforderlich ist. Dieser private digitale Schlüssel wurde bei der Einrichtung des Passkey-Zugriffs erstellt. Ebenso wurde bei der Einrichtung ein dazugehöriger öffentlicher digitaler Schlüssel erstellt. Mithilfe dieser beiden digitalen Schlüssel ist eine asymmetrische Kryptografie möglich. Und diese ist auch der Grund, weshalb Passkeys sicherer sind als Passwörter!

## So funktioniert Passkey vereinfacht




Ein Benutzer gibt auf der Anmeldeseite seinen Benutzernamen ein (Punkt 1). Der Server sendet nun eine lange Zahlenreihe an das Gerät des Benutzers, was als „Challenge“ (Herausforderung) bezeichnet wird (Punkt 2).

Das Gerät des Benutzers muss als Aufgabe den übermittelten Zahlencode mit dem privaten digitalen Schlüssel des Benutzers signieren. Damit das Gerät auf den privaten Schlüssel zugreifen kann, ist entweder die Eingabe einer PIN, ein Fingerabdruck oder Gesichtserkennung erforderlich. Im Anschluss wird der empfangene und signierte Zahlencode wieder an den Server gesendet (Punkt 3).

Der Server kann mithilfe des dazugehörigen öffentlichen Schlüssels überprüfen, ob der Zahlencode mit dem persönlichen Schlüssel signiert wurde. Ist das Ergebnis positiv, erhält der Benutzer Zugriff (Punkt 4).

## Deshalb sind Passkeys sicherer als Passwörter

Die Benutzer müssen sich nicht mehr für jeden Zugang ein Passwort überlegen und merken oder aufschreiben. Denn statt Passwörter wird ein digitales Schlüsselpaar verwendet, welches bei der Einrichtung erzeugt wird.

Der private Schlüssel bleibt beim Benutzer und nur der öffentliche Schlüssel wird auf dem Server gespeichert. Beim Anmeldevorgang werden nicht die Schlüssel ausgetauscht, sondern jedes Mal ein anderer Zahlencode. Der Server prüft bei der Rückmeldung, ob dieser Zahlencode mit dem passenden privaten Schlüssel signiert wurde. Somit müssten keine Passwörter auf dem Server gespeichert werden. Der öffentliche Schlüssel kann bislang nur dazu benutzt werden zu prüfen, ob der übermittelte Zahlencode mit dem privaten Schlüssel signiert wurde. Passwortdiebstahl und Phishing sowie geleakte Zugangsdaten wären damit weitestgehend nutzlos.

>

## > Der private Schlüssel des Nutzers

Der private Schlüssel ist also entscheidend für den Zugriff per Passkey und muss geschützt werden. Apple, Google und Microsoft haben hierfür entsprechende Anwendungen entwickelt und stellen diese in ihrem jeweiligen Ökosystem zur Verfügung. Alternativ ermöglichen auch einige Anbieter von Passwortmanagern, Passkey mit ihren Lösungen zu nutzen.

## Es gibt teilweise noch Herausforderungen

Wer die Geräte eines „Hersteller-Ökosystems" nutzt, also etwa Apple-Computer und iPhone, bekommt von der Verwaltung und dem Schutz nach der Einrichtung nicht viel mit. Die privaten Schlüssel werden sogar zwischen den Geräten synchronisiert. Bei der Passkey-Anmeldung öffnet sich ein Hinweis auf dem Computer oder Smartphone und fordert eine kurze Bestätigung, das heißt PIN, Gesichtserkennung oder Fingerabdruck, also die für viele Benutzer üblichen Anmeldemethoden, insbesondere an mobilen Geräten.

Wer Geräte unterschiedlicher Anbieter hat und im geschäftlichen Umfeld nicht auf ein Google-Konto in Verbindung mit dem Chrome-Browser zurückgreifen kann, der muss je nach individueller Situation die Anmeldung mit mehreren Geräten einrichten oder auf geräteübergreifende Passwort-/Passkey-Lösungen setzen.

Wer seine Passkeys nur auf einem Gerät hat, sollte zudem eine Datensicherung durchführen, damit er im Falle eines technischen Defekts oder Verlusts nicht auch noch seine Zugänge verliert.

Ein Sicherheitsproblem kann sein, dass einige Anbieter Passkey bislang nur als zusätzliche Option erlauben und parallel weiterhin ein Zugriff per Benutzername und Passwort möglich ist. Das kann langfristig zum Risiko werden, weil vermutlich viele im Laufe der Zeit das Passwort vergessen werden oder es möglicherweise nicht mitbekommen, wenn Dritte es haben und nutzen. Eine Schutzmaßnahme kann sein, solche Zugänge mit einem zweiten Faktor abzusichern.

## Gemeinsame Zugangsdaten und Notfallzugriff

In einigen Organisationen ist es teilweise noch erforderlich, dass mehrere Personen sich ein Konto „teilen" müssen. Das funktioniert mit Passkey nicht ohne Weiteres. Auch das zentrale Hinterlegen von Zugangsdaten – etwa als Notfalllösung – ist schwieriger. Hier sollten Unternehmen rechtzeitig klären, wie solche Konten künftig verwaltet werden können, insbesondere wenn Passkey zur einzigen Anmeldemöglichkeit wird.

## Diese Dienste bieten Passkey

Eine aktuelle Übersicht, welche Onlinedienste bereits Passkey unterstützen, finden Sie unter https://passkeys.directory. Über einen Klick auf „Details" beim entsprechenden Onlinedienst erhalten Sie direkt auch einen Link, an welcher Stelle Passkey eingerichtet werden kann, und Sie sparen sich die Suche in der Kontoverwaltung.

## So funktioniert die Einrichtung

Die Einrichtung von Passkey ist im Regelfall einfach und schnell erledigt. Nach einer normalen Anmeldung mit Benutzername und Passwort muss Passkey eingerichtet werden. Dies geschieht meistens durch einen Klick auf eine Schaltfläche. Der weitere Verlauf unterscheidet sich leicht je nach Anbieter, verwendetem Gerät und Passkey-Verwaltung.

Üblicherweise öffnet sich aber nach dem Klick auf die Schaltfläche ein neues Menüfenster auf dem Gerät. Über dieses Menü wird entweder der Speicherort abgefragt, womit sich die entsprechende Passkey-Verwaltung öffnet, oder es öffnet sich direkt die auf dem Gerät aktive Passkey-Verwaltung.

Diese Passkey-Verwaltung möchte dann eine PIN, den Fingerabdruck oder Gesichtserkennung. Damit ist die Einrichtung üblicherweise auch schon abgeschlossen. Bei der nächsten Anmeldung kann es noch erforderlich sein, Passkey als Anmeldeform auszuwählen. Dies wird aber üblicherweise beim Anmeldefenster angezeigt.

## Passkeys könnten viele Risiken minimieren

Passkeys sind eine vielversprechende Weiterentwicklung, die mittel- bis langfristig viele der bekannten Passwortprobleme lösen könnte. Zudem erspart sie einem die aufwendige Verwaltung von Zugangsdaten. Einmal eingerichtet, funktioniert diese Art der Anmeldung einfach und sicher. Erkundigen Sie sich bei Ihren internen Ansprechpartnern, ob und wie Passkeys in Ihrem Unternehmen eingesetzt werden dürfen. Auch für private Zugänge kann Passkey eine sinnvolle Alternative zum Passwort sein. Falls Sie ein Unternehmens-Smartphone haben, denken Sie aber bitte daran, Ihre persönlichen digitalen Schlüssel auch an anderen Stellen zu speichern, damit Sie nicht Ihre Zugänge verlieren, wenn die Geräte etwa ausgetauscht werden (ST)

# „NICHT MEIN GERÄT, NICHT MEIN PROBLEM?“ – DATENSCHUTZ BEIM TEILEN VON ARBEITSMITTELN

**Sie kennen das: Der eigene Laptop ist gerade im Update-Fieber, also wird kurzerhand der Rechner vom Kollegen benutzt – „nur ganz kurz, nur zum Ausdrucken“. Oder das Kundentelefonat wird fix am Platz der Kollegin geführt, weil das Headset dort einfach besser klingt. Und überhaupt: In Zeiten von Wechselarbeitsplätzen, geteilten Geräten und flottem Teamwork ist es längst normal, dass nicht immer nur einer vor einer Tastatur sitzt. Flexibilität ist das Thema der Stunde – aber was macht eigentlich der Datenschutz dabei?**

So praktisch das Teilen von Arbeitsmitteln im Alltag ist, so tückisch kann es werden, wenn niemand so genau weiß, wer da gerade mit wessen Zugangsdaten arbeitet oder welche sensiblen Informationen auf dem Bildschirm noch sichtbar sind. Ganz zu schweigen von dem USB-Stick, der „mal schnell“ angeschlossen wird – auf einem Gerät, das eigentlich jemand anderem gehört. Klingt banal? Ist es leider nicht. Denn genau in diesen kleinen Momenten entstehen oft die großen Datenschutzpannen – nicht aus böser Absicht, sondern aus Unachtsamkeit.

Deshalb geht es heute nicht um Verbote oder Vorschriften, sondern um den gesunden Menschenverstand im digitalen Miteinander. Wir zeigen Ihnen, worauf Sie beim Teilen von Geräten, Zugängen oder Arbeitsplätzen achten sollten – mit konkreten Tipps, einer kompakten Checkliste und ein paar Schmunzlern aus dem Büroalltag. Denn Datenschutz funktioniert am besten, wenn alle mitdenken – egal an welchem Schreibtisch.

## „Nur mal kurz …“ – und schon ist’s passiert

Die meisten Datenschutzpannen beim Teilen von Arbeitsmitteln passieren nicht, weil jemand Regeln missachtet, sondern weil es schnell gehen muss. „Nur mal eben“ – das ist die wohl gefährlichste Aussage im Büroalltag. Denn egal ob Notebook, Telefon oder Softwarezugang: Sobald mehrere Personen dieselbe Hardware oder denselben Account nutzen, wird es unübersichtlich – und potenziell unsicher.

Typische Stolperfallen aus dem Alltag:

- **Offene Arbeitsplätze, offene Geheimnisse:** Beim sogenannten Desksharing kann der nächste Kollege schon am Platz sitzen, bevor der vorherige sich vollständig abgemeldet hat. Ist der Bildschirm noch entsperrt? Liegt der Ausdruck mit den vertraulichen Vertragsdetails noch auf dem Tisch? Datenschutz findet auch zwischen zwei Schichten statt.
- **Gemeinsame Benutzerkonten:** Ob im Lager-PC oder an der Rezeption – wenn mehrere Mitarbeitende denselben Log-in verwenden, weiß hinterher niemand mehr, wer wann was gemacht hat. Für die IT-Sicherheit ist das ein Albtraum – für die Nachvollziehbarkeit im Ernstfall auch.
- **Zugänge, die wanderfreudig sind:** „Ich brauch mal deinen Zugang zur Software – nur kurz!“ klingt harmlos, ist aber heikel. Wer sein Passwort teilt, gibt nicht nur Zugriff, sondern im Zweifelsfall auch Verantwortung ab. Und die landet spätestens bei einer Datenpanne genau dort, wo sie keiner haben will.
- **Geteilte Geräte, geteilte Daten:** Wenn das Diensthandy der Abteilung mal eben an eine Aushilfe weitergereicht wird oder mehrere Personen ein Tablet nutzen – ohne klare Trennung der Daten und Benutzer wird’s schnell unübersichtlich. Und manchmal bleiben Kundendaten da, wo sie niemand erwartet.

## 5 Punkte, auf die Sie konkret achten sollten:

1. Melden Sie sich immer vom System ab, wenn Sie den Arbeitsplatz verlassen – selbst wenn’s „nur fünf Minuten“ sind.
2. Verwenden Sie keine gemeinsam genutzten Accounts – jede Person braucht einen eigenen Zugang mit individuellen Rechten.
3. Teilen Sie keine Passwörter – auch nicht „nur einmal kurz“ und auch nicht mit dem nettesten Kollegen.
4. Nutzen Sie, wenn möglich, Geräte mit Nutzerprofilen oder Sperrfunktionen, um private und dienstliche Daten sauber zu trennen.
5. Klären Sie im Team: Wer darf welches Gerät wie nutzen – und was passiert mit sensiblen Daten danach?

>

## > Ein USB-Stick, ein Kaffee und das große Rätsel

Es war ein ganz normaler Dienstagmorgen, als Marie ins Büro kam. Auf ihrem Schreibtisch: ein fremder USB-Stick. Daneben ein gelber Post-it mit der kryptischen Nachricht: „Da sind die Unterlagen für die Präsentation drauf. Danke! – T."

Marie runzelte die Stirn. Ein Stick? Einfach so? Ohne Hülle, ohne Absender, ohne Warnung? Neugierig – aber auch etwas nervös – steckte sie das Ding in ihren Laptop.

Nichts passierte. Keine Datei. Kein Ordner. Nur eine Fehlermeldung. Und dann … ein flackernder Bildschirm. Die IT war schnell zur Stelle und konnte Schlimmeres verhindern. Aber der Stick hatte bereits versucht, Schadsoftware zu installieren – gut getarnt hinter einem vermeintlichen Präsentationsdokument.

### Mein Tipp:

Der „Kollege T." war übrigens ein neuer Praktikant, der sich nicht sicher war, wie man Dateien im Netzwerk freigibt – und stattdessen zum „altbewährten" Stick griff. Dass er dabei fast das halbe Netzwerk lahmgelegt hätte, war ihm ehrlich peinlich. Die Moral von der Geschicht? Geteilte Arbeitsmittel brauchen klare Spielregeln – für alle.

## Wenn plötzlich „Sie" eine E-Mail schreiben, die Sie nie getippt haben

Stellen Sie sich vor, Sie kommen morgens ins Büro, schalten Ihren Rechner ein – und werden von einem leicht nervösen Kollegen begrüßt: „Du, danke noch mal für die Mail gestern Abend. Harter Ton, aber du hast recht – das mit dem Projekt war wirklich schiefgelaufen." Sie stutzen. Mail? Abends? Projekt? Sie hatten gestern um 17 Uhr das Büro verlassen und sind mit gutem Gewissen ins Fitnessstudio. Kein Laptop, kein Handy, kein „Nur noch mal schnell nachschauen". Sie öffnen Ihr Postfach – und da ist sie: eine E-Mail, gesendet von Ihrem Account, voller Details und Vorwürfe, die Sie nie formuliert haben. Was ist passiert?

**Die bittere Wahrheit:** Ihr Rechner stand offen. Vielleicht nicht einmal absichtlich – vielleicht war's nur ein vergessener Sperrbildschirm. Vielleicht war auch Ihr Passwort gespeichert oder auf einem Zettel im Schreibtisch. Jemand hat sich Zugriff verschafft. Und jemand hat in Ihrem Namen geschrieben.

## Und jetzt? Jetzt wird's unangenehm

Denn wenn eine E-Mail mit Ihrem Absender verschickt wurde, gelten Sie als der Urheber. In den Logfiles steht Ihr Benutzername, nicht der Name der tatsächlichen Person, die an Ihrem Platz saß. Für die IT ist das eindeutig – und im Zweifelsfall auch für Vorgesetzte, den Betriebsrat oder – wenn's ganz dumm läuft – die Rechtsabteilung.

## Beweislast? Schwierig

Je nach Unternehmensrichtlinie müssen Sie jetzt glaubhaft darlegen, dass Sie es nicht waren. Und das ist verdammt schwer, wenn es keine Protokollierung, keine Kamera, keine Sperre oder wenigstens eine saubere Benutzertrennung gab.

## Und wenn's noch schlimmer kommt? Diese Risiken müssen Sie kennen

Nehmen wir an, nicht nur eine E-Mail wurde geschrieben, sondern jemand hat auch vertrauliche Dokumente kopiert, sensible Daten gelöscht oder in ein externes Postfach weitergeleitet. Vielleicht sogar mit böswilliger Absicht – ein interner Konflikt, ein Rache- >

akt oder einfach Unachtsamkeit. Der Schaden ist real – und Sie stehen mit Ihrem Namen drin.

**Mein Tipp:**
Und der gute alte USB-Stick? Dasselbe Spiel. Wenn Sie einen fremden Stick in Ihren Dienst-Laptop stecken und darüber unbemerkt Schadsoftware ins Netzwerk bringen, landen Sie ganz schnell im Fokus. Es hilft dann nicht zu sagen: „Ich wollte doch nur helfen …" – gut gemeint ist im Datenschutz leider nicht gleich gut gemacht.

## Was lernen wir daraus? 3 Punkte, die Sie wissen müssen

1. Persönliche Zugänge sind wie Unterschriften. Sie belegen, dass Sie gehandelt haben. Oder zumindest dafür verantwortlich waren, was auf Ihrem Account passiert ist.
2. Wer Geräte nicht absichert, lädt (unfreiwillig) zum Missbrauch ein.
3. „Nur kurz mal ausgeliehen", kann teuer werden – für das Unternehmen, aber auch für Sie persönlich.

## Fazit: Datenschutz schützt auch Sie – wenn Sie mitspielen

Am Ende geht es beim Datenschutz nicht um Paragrafenreiterei, Bürokratie oder nervige IT-Regeln. Es geht um Vertrauen. Und um Sicherheit – Ihre eigene, die Ihrer Kolleginnen und Kollegen – und die des gesamten Unternehmens.

Denn klar ist: Wer seine IT-Geräte offen lässt, sein Passwort teilt oder „nur mal schnell" fremde USB-Sticks nutzt, hat meist keine bösen Absichten.

Aber auf Absichten kommt es im Ernstfall nicht an – sondern auf Verantwortung. Und die tragen Sie für Ihren Zugang, Ihre IT-Geräte und Ihre Arbeitsweise. Datenschutz ist dabei kein Papiertiger, der in der Schublade vor sich hin staubt.

Er ist Ihr Schutzschild – vor Missverständnissen, vor Fehlbeschuldigungen, vor echten Schäden. Wer achtsam mit seinen Datenzugängen umgeht, schützt nicht nur Unternehmens- und Kundendaten, sondern auch sich selbst.

Also bitte: Sperren Sie Ihren Bildschirm. Behalten Sie Ihre Zugangsdaten für sich. Und sagen Sie beim nächsten „Darf ich mal kurz an deinen Rechner?" vielleicht einfach freundlich: „Klar, wenn du dich mit deinem eigenen Zugang anmeldest."

## Meine Empfehlung:

Denken Sie immer daran: Geteilte Geräte sind okay. Aber Verantwortung – die ist nicht teilbar. (AH)

# WUSSTEN SIE SCHON, DASS IHR DRUCKER EIN GEDÄCHTNIS HAT?

**Einfach ausdrucken, fertig – und das Papier ist weg. Aber was ist mit den Daten? Viele moderne Drucker und Multifunktionsgeräte sind kleine Computer: mit Speicher, Festplatte oder Cloud-Anbindung. Und genau hier liegt die Überraschung.**

Denn was viele nicht wissen: Die meisten Geräte speichern Kopien der gedruckten, gescannten oder gefaxten Dokumente – oft über Wochen oder Monate. Das mag bei der Urlaubsplanung kein Problem sein. Aber wenn es um sensible Kundendaten, interne Verträge oder Gehaltsabrechnungen geht, wird's kritisch.

Das Risiko? Beim Weiterverkauf oder der Entsorgung solcher Geräte landen diese Daten schlimmstenfalls beim nächsten Besitzer – inklusive der letzten 100 Ausdrucke. Auch ein unbeaufsichtigter Drucker im Büro kann so zur Datenfalle werden.

Was können Sie tun?

- Vor dem Ausmustern: Lassen Sie den Speicher professionell löschen oder zurücksetzen.
- Im Betrieb: Holen Sie Ausdrucke zeitnah ab – besonders bei Sammeldruckern.
- Im Zweifel: Fragen Sie Ihren IT-Support, ob Ihr Gerät über eine Löschfunktion verfügt.

**Kleiner Tipp am Rande:** Auch Kopierer zählen zu den heimlichen Datensammlern. Sie merken schon – Datenschutz fängt manchmal dort an, wo man ihn am wenigsten vermutet. (AH)

# 5 KLEINE GEWOHNHEITEN MIT GROSSER WIRKUNG FÜR MEHR DATENSICHERHEIT UND DATENSCHUTZ

Nicht immer sind es technisch raffinierte Hacking-Angriffe, welche für Stress und Kosten bei Unternehmen sorgen. Manchmal reicht hierfür eine einzelne Person. Aber mit 5 kleinen Gewohnheiten können Sie das Risiko im Arbeitsalltag erheblich reduzieren.

In unserem Video haben wir diese für Sie gesammelt. Scannen Sie dafür einfach den QR-Code und teilen Sie das Video auch gerne mit Ihren Kollegen.

## Ich habe die Ausgabe von Privacy@Work gelesen:

| Name, Vorname, Abteilung | Unterschrift |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

**Bei Fragen im Bereich Datenschutz wenden Sie sich bitte an Ihre Datenschutzbeauftragte oder Ihren Datenschutzbeauftragten!**


## Impressum:

PRIVACYXPERTS

PrivacyXperts, ein Unternehmensbereich der VNR Verlag für die Deutsche Wirtschaft AG, Theodor-Heuss-Straße 2–4, D-53177 Bonn; Großkundenpostleitzahl: D-53095 Bonn; Handelsregister: HRB 8165, Registergericht: Amtsgericht Bonn, Vertreten durch den Vorstand: Richard Rentrop, ISSN: 1614 – 5674; Kontakt: Telefon: 0228 – 9 55 01 60 (Kundendienst); Telefax: 0228 — 3 69 64 80, E-Mail: kundendienst@privacyxperts.de, Internet: https://www.privacyxperts.de, Umsatzsteuer: Umsatzsteuer-Identifikationsnummer gemäß §27a Umsatzsteuergesetz: DE 812639372, V.i.S.d.P.: Michael Jodda; Theodor-Heuss-Straße 2–4; D-53177 Bonn, Herausgeber: Michael Jodda, Bonn, Autoren: Andreas Hessel, Sebastian Tausch, Produktmanagement: Lisa Greiling, Bonn, Layout & Satz: Bettina Pour-Imani, BB-Design, Birken-Honigsessen, Bildrechte Seite 1: tanit – AdobeStock.com, Druck: Warlich Druck Meckenheim GmbH, Meckenheim

Erscheinungsweise: 16-mal pro Jahr; Im Interesse der Lesbarkeit verzichten wir in unseren Beiträgen auf geschlechtsbezogene Formulierungen. Selbstverständlich sind immer Frauen und Männer gemeint, auch wenn explizit nur eines der Geschlechter angesprochen wird. Alle Angaben in Privacy@Work wurden mit äußerster Sorgfalt ermittelt und überprüft. Sie basieren jedoch auf der Richtigkeit uns erteilter Auskünfte und unterliegen Veränderungen. Eine Gewähr kann deshalb nicht übernommen werden.

Dieses Produkt besteht aus FSC®-zertifiziertem Papier