

**Mit Phishing-
Resistant-MFA und
Passkeys gegen
MiTM-Attacken
bestens geschützt**



Alexander Karls
Cloud- und Security-Consultant
Mail: a.karls@pegasus-gmbh.de
Tel.: +49 9402 503-214

Kurzprofil:

- ✦ Über 20 Jahre in der IT tätig
- ✦ Mehr als 15 Jahre Erfahrung in leitender Funktion
- ✦ Langjährige Erfahrung aus selbständiger Tätigkeit
- ✦ Vorfall-Experte im CSN des BSI
- ✦ Erfahrener Trainer und Coach
- ✦ Podcast-Host von BlueScreen – Der Tech-Podcast



Mitarbeiterzahl	100
Zertifizierung	ISO 9001 / 27001 / 27018
Standorte	Regenstauf (pegasus GmbH / pegasus IT / IQ) Ludwigsburg (EVIATEC Systems AG) Bern (EVIATEC Digital Solutions AG) Brøndby / Kopenh. (EVIATEC Scandinavia ApS)
Rechenzentren	3
Einsatzgebiet	Europaweit / Weltweit
Vernetzung	> 1500 Standorte weltweit
Geschützte Anwender	> 50.000
Server im RZ	> 500
Kundengröße / Schnitt	25 - 1000



Regensburg / DE



Ludwigsburg / DE



Bern / CH



Kopenhagen / DK

Zeit für ein Quiz!

Wieviele Prozent aller Angriffe basieren auf Phishing?

Wieviel Prozent aller Angriffe basieren auf Phishing?



Cybercrime Statistics 2024



\$10.5 Trillion

projected cost of cybercrimes by 2025.



\$1.5 Trillion

Amount earned by cybercriminals for cybercrime activities yearly.



\$5.09 Million

Is the highest cost of a data breach in U.S.A. in 2023.



\$30 billion

Cost of Crypto-crime annually by 2025.



80%

of cybercrimes are phishing attacks in the technology sector.



2.7 billion hours

Total time spent resolving cybercrimes; average of 6.7 hours daily.

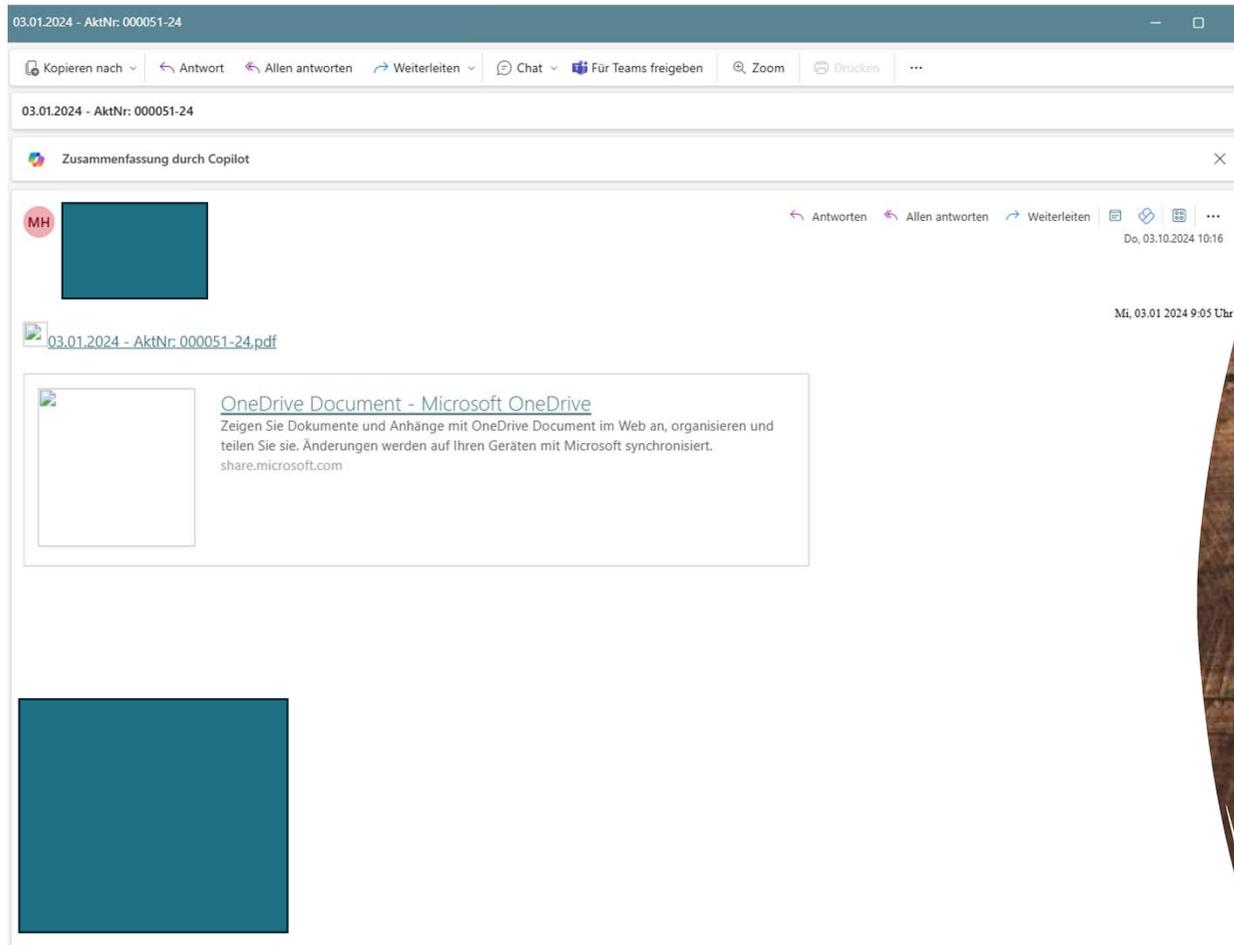
\$265 Billion

is the estimated annual cost of ransomware to victims by 2031.



„Ich habe nichts gemacht und auf einmal war alles kaputt!“

Das Problem – Eintrittsvektor E-Mail



Das Problem – Umleitung zu „OneDrive“ > Canva



Die [redacted] GmbH hat Ihnen ein neues Dokument zur Verfügung gestellt.

DOKUMENT: AW240098

DATUM: Donnerstag, 3. Oktober 2024

Eine PDF-Datei des Dokuments finden Sie im Scan.

[DOKUMENT ANZEIGEN](#)



But first, cookies 🍪

We use essential cookies to make Canva work. We'd like to use other cookies to improve and personalize your visit, tailor ads you see from us on Canva and partner sites, and to analyze our website's performance, but only if you accept. Learn more about your choices in our cookie policy.

[Accept all cookies](#) [Reject all cookies](#) [Manage cookies](#)

Datenschutzerklärung

<https://www.canva.com/link?target=https://xzl5ivdazwobdg6qmgjvaqcpwbgzcdsuwpt3rzsgejp>

Das Problem – Erste Login-Versuche



Authentifizierungsmethoden | Richtlinien > Benutzer > Multi-Faktor-Authentifizierung pro Benutzer > Benutzer > Sicherheit | Riskante Anmeldungen > Benutzer

Benutzer | Anmeldeprotokolle

Microsoft Entra ID

Suche

Herunterladen | Dateneinstellungen exportieren | Problembehandlung | Aktualisieren | Spalten | Haben Sie Feedback für uns?

Diese Ansicht wird bald durch eine Ansicht ersetzt, die Aktualisierungstoken und Anwendungsanmeldungen enthält. Testen Sie unsere Vorschau für neue Anmeldungen. →

Datum: **Letzte 7 Tage** | Datum anzeigen als: **Lokal** | Filter hinzufügen

Datum	Anforderungs-ID	Benutzer	Anwendung	Status	IP-Adresse	Standort
1.10.2024, 21:06:57				Unterbrochen		DE
1.10.2024, 21:05:48				Erfolg		Muenchen, Bayern, DE
1.10.2024, 17:55:24				Unterbrochen		Leipzig-Zentrum-Sued, Sachsen, DE
1.10.2024, 16:58:23				Unterbrochen		Leipzig-Zentrum-Sued, Sachsen, DE
1.10.2024, 14:28:31				Erfolg		Leipzig-Zentrum-Sued, Sachsen, DE
1.10.2024, 12:09:29				Erfolg		Leipzig-Zentrum-Sued, Sachsen, DE
1.10.2024, 11:29:36				Unterbrochen		Leipzig-Zentrum-Sued, Sachsen, DE
1.10.2024, 11:29:32				Unterbrochen		Leipzig-Zentrum-Sued, Sachsen, DE
1.10.2024, 11:27:50				Unterbrochen		Leipzig-Zentrum-Sued, Sachsen, DE
30.9.2024, 22:01:55				Unterbrochen		DE
30.9.2024, 19:55:58				Erfolg		Muenchen, Bayern, DE
30.9.2024, 11:53:06				Erfolg		Wolferstadt, Bayern, DE
30.9.2024, 10:57:16				Erfolg		Leipzig-Zentrum-Sued, Sachsen, DE
29.9.2024, 03:15:24				Fehler		Kampung Tekir Mentera, Negeri Sembilan, MY
28.9.2024, 18:10:00				Erfolg		DE
28.9.2024, 17:03:21				Fehler		Kampung Paya Kenangan, Johor, MY
27.9.2024, 16:44:07				Erfolg		Leipzig-Zentrum-Sued, Sachsen, DE
27.9.2024, 15:23:34				Unterbrochen		DE
27.9.2024, 15:21:42				Erfolg		DE
27.9.2024, 09:02:32				Erfolg		Leipzig-Zentrum-Sued, Sachsen, DE

Das Problem – Treffer!



Details zu Risikobenzern



[Kennwort zurücksetzen](#) [Benutzergefährdung bestätigen](#) [Benutzer als sicher bestätigen](#) ...

Grundlegende Infos **Letzte riskante Anmeldungen** Erkennungen ohne Bezug zu einer Anmeldung Risikoverlauf

Anwendung	Status	Datum	IP-Adresse	Standort	Risikozust
OfficeHome	Erfolg	3.10.2024, 08:55:58	84.239. [redacted]	Baltimore, Maryland, US	Gefährdet
OfficeHome	Unterbrochen	3.10.2024, 08:55:55	84.239. [redacted]	Baltimore, Maryland, US	Gefährdet

Für Benutzer können Erkennungen zu Anmeldungen vorliegen, die im Bericht für Anmeldungen aktuell nicht unterstützt werden. Solche riskanten Anmeldungen werden hier nicht angezeigt. Um alle Erkennungen der letzten 90 Tage anzuzeigen, wechseln Sie zur Registerkarte "Risikoverlauf".

84.239. [redacted]

Summary Resolutions **WHOIS** Certificates Trackers Components Host pairs Cookies Services Reverse DNS Articles Profiles Projects

Records by date

Extended WHOIS history records are only available to licensed account holders. [Learn more](#)

WHOIS record: 2023-04-25

Record updated: 2023-04-25 | Last scanned: 2024-10-01 | Expiration: Expiration N/A | Created: over 1 year ago

Values Raw

Attribute	Value
WHOIS server	rdap.db.ripe.net
Registrar	RIPE
Domain status	active
Email	abuse@invitesys.ro - (abuse) abuse@invitesys.ro.noc@adnettelecom.ro - (tech, admin)
Name	INVITE Systems - (tech, admin) Abuse-C Role - (abuse) MNT-ADNET - (registrant)
Organization	-
Street	nr. 1/vi bloc 1 sos. pipera-tunari.et. 4 - (abuse) 1/vi blvd ilfov - (tech, admin)
City	voluntari - (tech, abuse, admin)
State	-
Postal code	077190 - (abuse)
Country	romania - (abuse)
Phone	-
Nameservers	-

Red Flags – everywhere!



Eine PDF-Datei des Dokuments finden Sie im Scan.

[DOKUMENT ANZEIGEN](#)

03.01.2024 - AktNr. 000051-24.pdf



[OneDrive Document - Microsoft OneDrive](#)

Zeigen Sie Dokumente und Anhänge mit OneDrive Document im Web an, organisieren und teilen Sie sie. Änderungen werden auf Ihren Geräten mit Microsoft synchronisiert.
share.microsoft.com

<https://www.canva.com/link?target=https://xz15ivdazwobdg6qmgjvaqcpwbgzcdsuwpqt3rzwsgjep>

„Wie machen
die Angreifer
das?“

This is how they do it! Also, so oder so ähnlich ;)



The screenshot shows the DeHashed search interface in a Mozilla Firefox browser. The search query is '@tesla.com'. The results page displays the following statistics:

- 473 RESULT(S) FOUND
- 169MS SEARCH ELAPSED TIME
- 12,387,953,776 ASSETS SEARCHED
- 24,552 AGGREGATED DATA WELLS

The results section is titled 'Results:' and includes a disclaimer: 'Because of the nature of the displayed data, no guarantee can be and/or is made regarding its accuracy.' The results are listed as follows:

- george@tesla.com**
Sourced from ShareThis data
Request entry removal
- Safety@Tesla.com**
Sourced from ShareThis data
Request entry removal
- Tesla@tesla.com**
Sourced from ShareThis data

On the right side, there is a section titled 'What's DeHashed and those results?' which explains that DeHashed is a public data search-engine created for Security Analysts. It shows a specific result entry:

Result #240834786

Name	george@tesla.com
Email	george@tesla.com
Username	fc458d6f4759d2799286dda8

Below the table, there is a note: 'Simply click on request entry removal below results and complete the automated on-screen process.'

This is how they do it! Also, so oder so ähnlich ;)



This is how they do it! Also, so oder so ähnlich ;)



The screenshot displays the Gophish website. The main heading is "Open-Source Phishing Framework". Below it, a sub-heading states: "Gophish is a powerful, open-source phishing framework that makes it easy to test your organization's exposure to phishing." Below this, it says "For free." and provides two buttons: "Download" and "Learn More".

The website also features a navigation bar with links for "Documentation", "Support", "Blog", and "Download".

The central part of the image shows a laptop displaying the Gophish dashboard. The dashboard includes a "Dashboard" section with a line graph showing a fluctuating trend. Below the graph are four circular progress indicators for "Email Sent", "Email Opened", "Clicked Link", and "Submitted Data". The "Recent Campaigns" section shows a list of campaigns with colored bars representing their status.

Demo Gophish



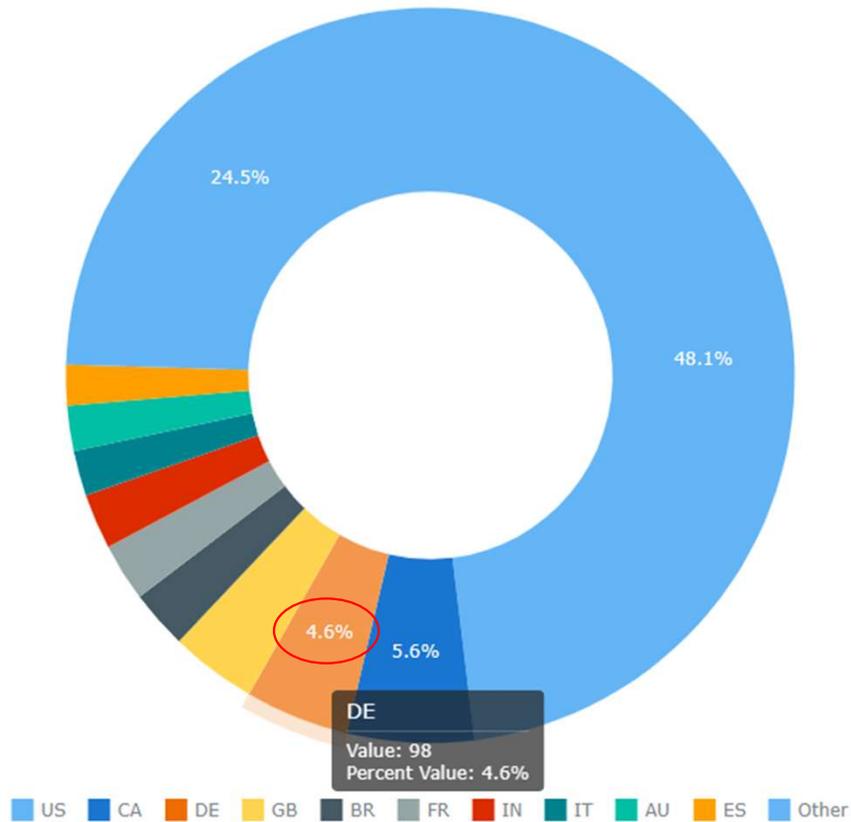
Zeit für ein Quiz!

Welchen Platz
belegt
Deutschland bei
Ransomware in
2025?

Welchen Platz belegt Deutschland bei Ransomware in 2025?



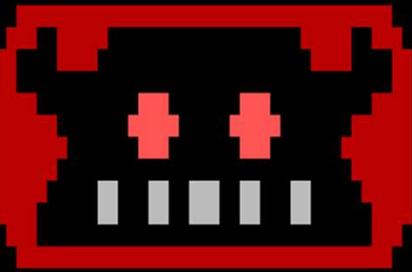
🌍 Top 10 Victim countries for 2025





This is how they do it! Also, so oder so ähnlich ;)

```
root@debian-evilginx:~/tools/evilginx2# ./build/evilginx -p ./phishlets/
```



```
no nginx - pure evil
by Kuba Gretzky (@mrgretzky) version 2.0.0
```

```
[08:23:56] [inf] loaded phishlet 'google' from 'google.yaml'
[08:23:56] [inf] setting up certificates for phishlet 'google'...
[08:23:56] [^*] successfully set up SSL/TLS certificates for domains: [accounts.it-is-almost-done.evilginx.com apis.it-is-almost-done.evilginx.com ssl.it-is-almost-done.evilginx.com content.it-is-almost-done.evilginx.com]
[08:23:59] [imp] [0] new visitor has arrived: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36
[08:23:59] [inf] [0] landing URL: https://accounts.it-is-almost-done.evilginx.com/signin/v2/identifier
: sessions
```

id	phishlet	username	password	tokens	remote ip	time
19	google			none	[REDACTED]	2018-05-28 08:23

```
[08:24:22] [^*] [0] Username: [REDACTED]@gmail.com
[08:24:29] [^*] [0] Password: [REDACTED]
[08:24:41] [^*] [0] all authorization tokens intercepted!
[08:24:41] [imp] [0] redirecting to URL: https://redirect-to-this-url-after-logging-in.com
: sessions
```

id	phishlet	username	password	tokens	remote ip	time
19	google	[REDACTED]@gmail.com	[REDACTED]	captured	[REDACTED]	2018-05-28 08:24

This is how they do it!



🔗 Evilginx 3.0

Evilginx is a man-in-the-middle attack framework used for phishing login credentials along with session cookies, which in turn allows to bypass 2-factor authentication protection.

This tool is a successor to [Evilginx](#), released in 2017, which used a custom version of nginx HTTP server to provide man-in-the-middle functionality to act as a proxy between a browser and phished website. Present version is fully written in GO as a standalone application, which implements its own HTTP and DNS server, making it extremely easy to set up and use.

<https://github.com/kgretzky/evilginx2>

„Aber wir haben doch MFA?“



Bad: Password

123456
Qwertz
password
P@ssw0rd
iloveyou
Sars-Cov-2
Covid-19

Good: Password +



SMS



Voice

Better: Password +



Push
Notification



Soft
Tokens OTP



Hard
Tokens OTP

Best:



Microsoft
Authenticator

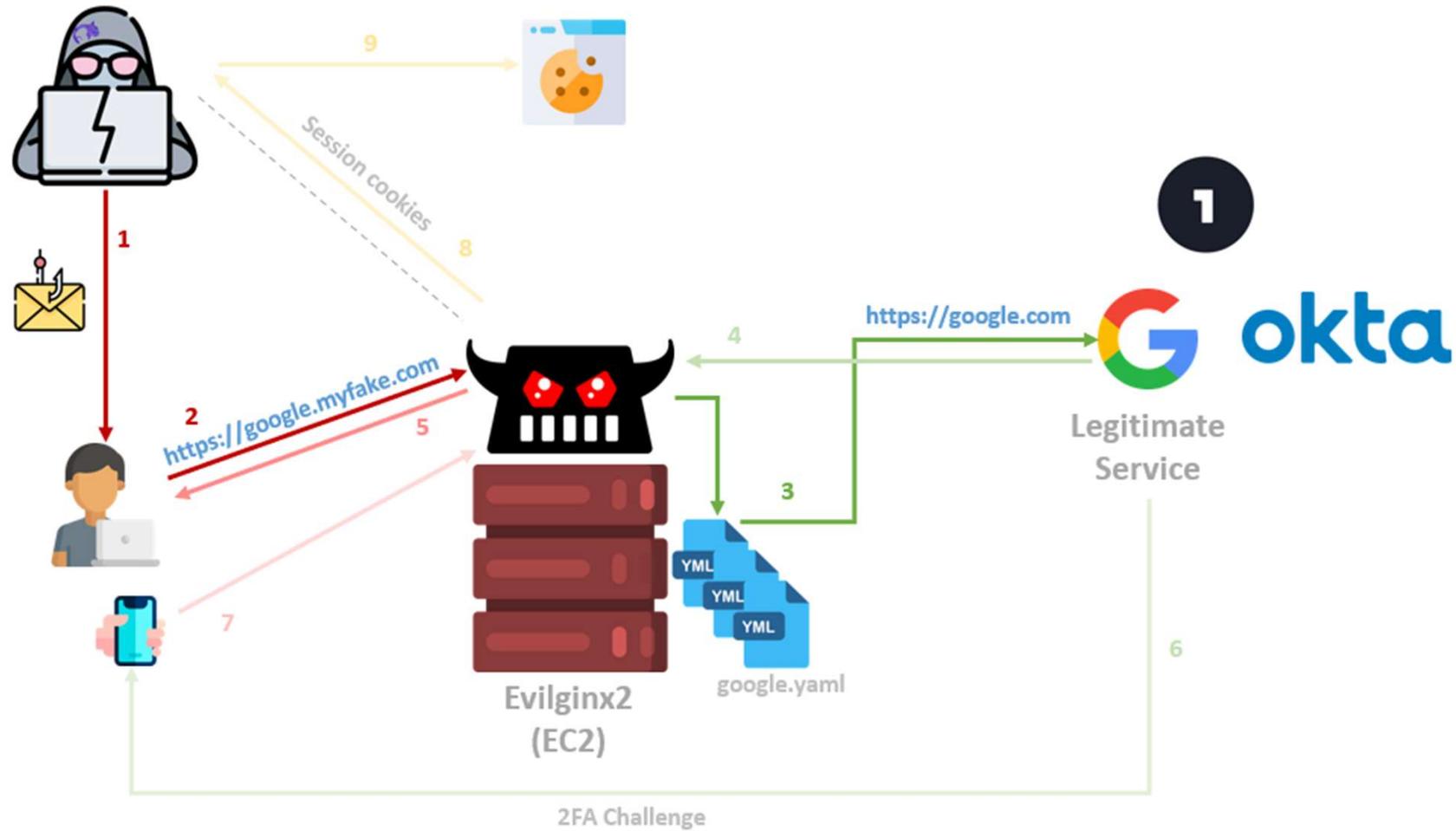


Windows
Hello



FIDO2
Security key

Technische Details



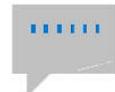
„Aber wir haben doch MFA?“



Bad: Password

123456
Qwertz
password
P@ssw0rd
iloveyou
Sars-Cov-2
Covid-19

Good: Password +



SMS



Voice

Better: Password +



Push
Notification



Soft
Tokens OTP



Hard
Tokens OTP

Best:



Microsoft
Authenticator



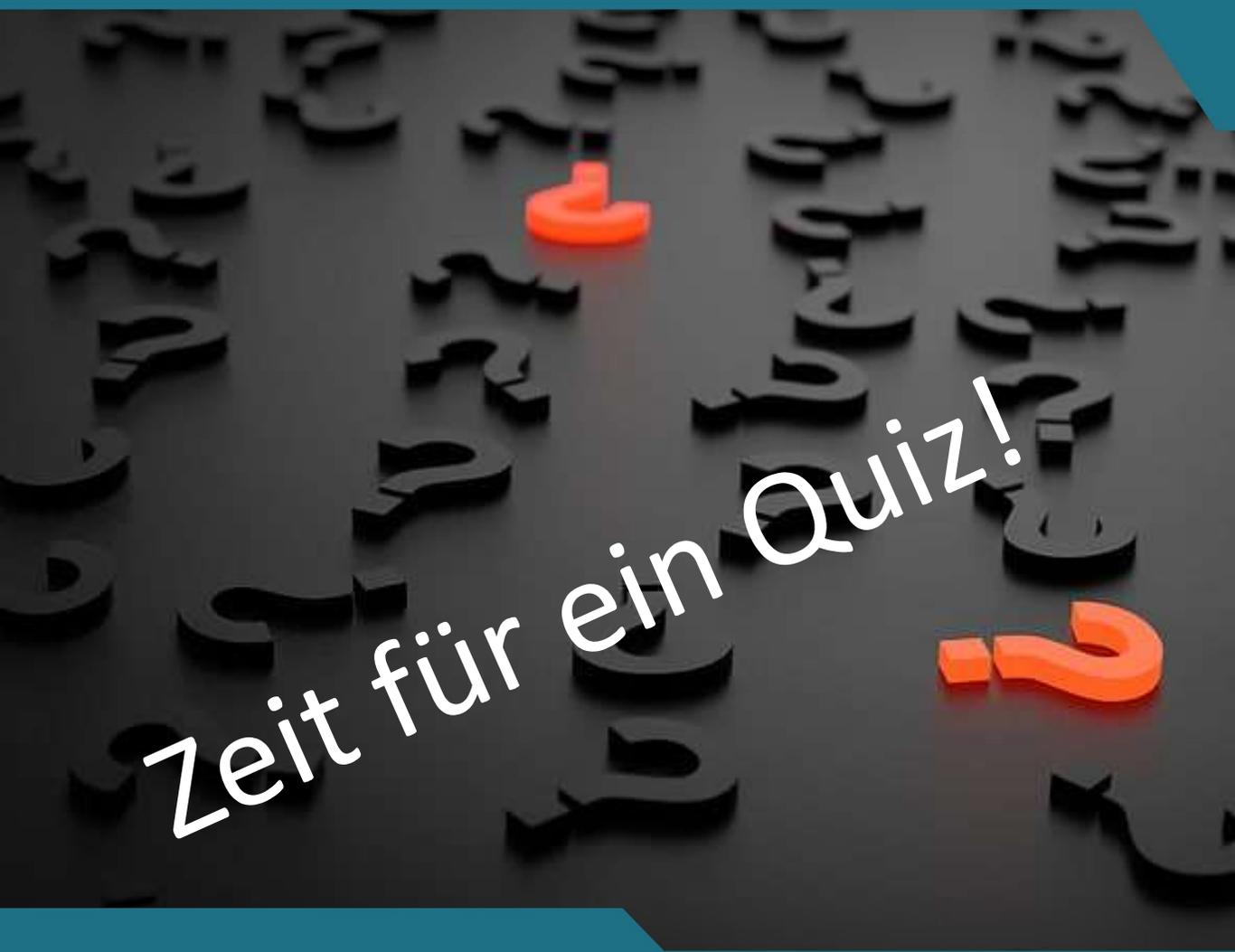
Windows
Hello



FIDO2
Security key

Phishing-Resistant MFA!

Demo EvilGinx



Zeit für ein Quiz!

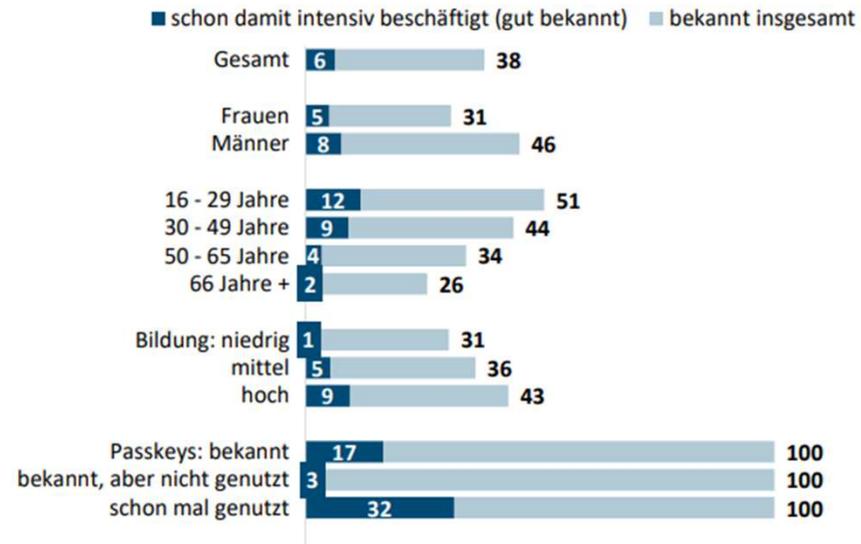
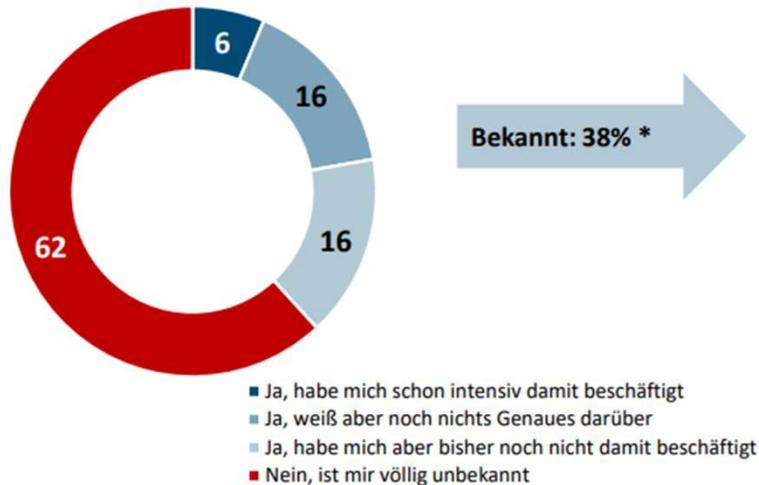
Wer kann mit dem Begriff „Passkey“ etwas anfangen?



Wer kann mit dem Begriff „Passkey“ etwas anfangen?

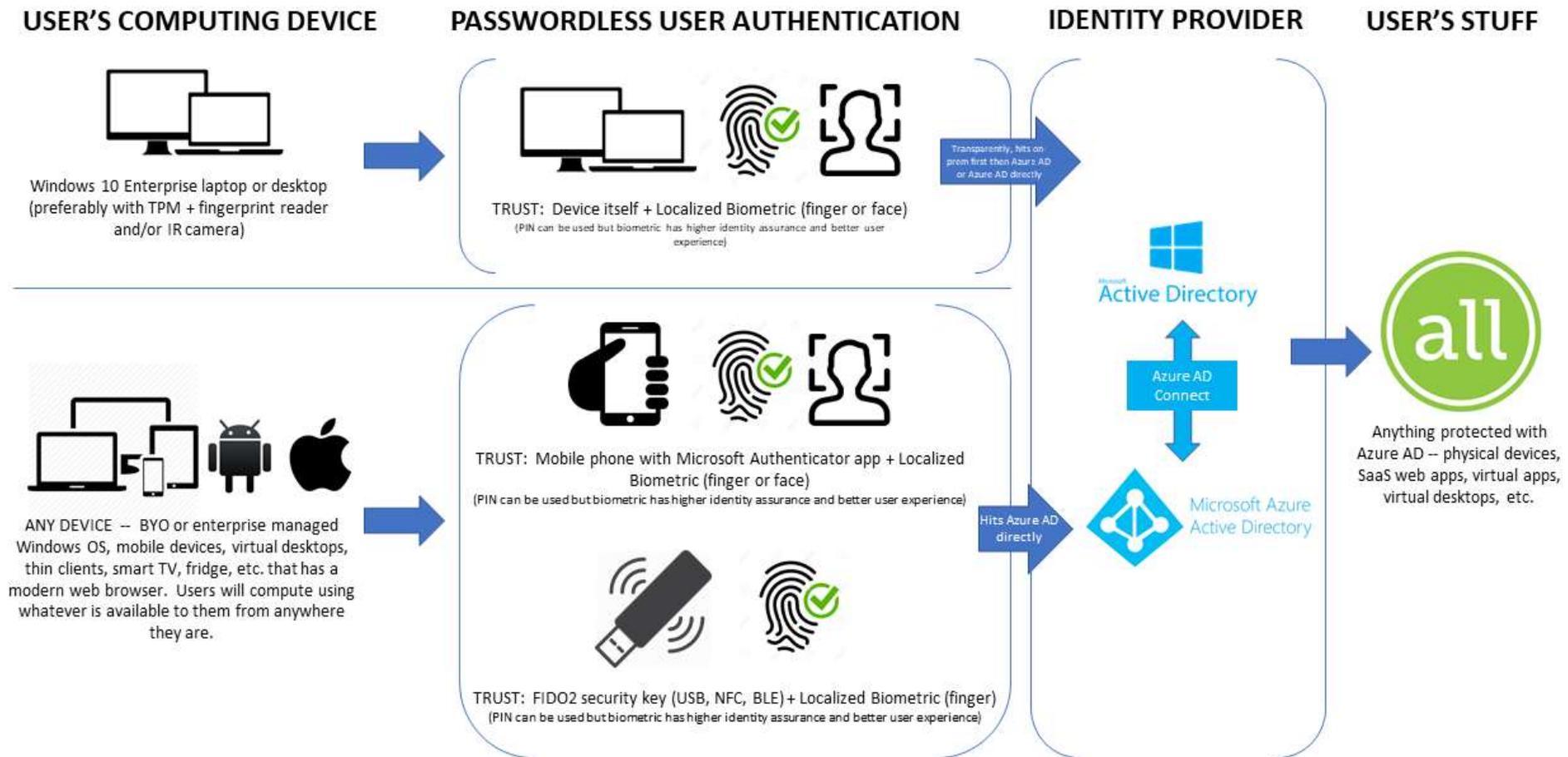
Passkeys: Gestützte Bekanntheit (nach Beschreibung)

Über einem Drittel ist Passkeys zumindest vom Begriff her bekannt. Von den Passkeys-Nutzenden hat sich die überwiegende Mehrheit noch nicht intensiv damit beschäftigt.



PK2. Kennen Sie diese Möglichkeit, sich mit Passkeys bei Online-Diensten und deren Apps anzumelden?
Basis: Gesamt n= 1.519 | Angaben in %, * Die Selbsteinschätzung wird evtl. nicht mit den realen Anteilen übereinstimmen.

Passkeys / Hardware-Based Authentication



Token-Hardware (Bsp. Yubikey)



Token-Hardware (Bsp. Yubikey)



Microsoft | Konto Ihre Informationen Datenschutz Sicherheit Rewards Zahlung und Abrechnung Mehr

Sicherheitsschlüssel einrichten

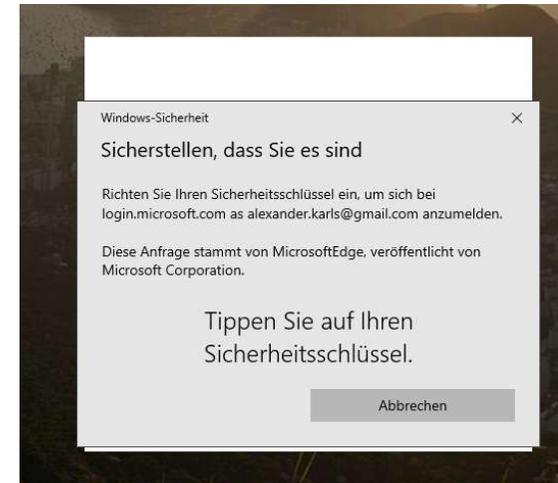
Schlüssel bereithalten

 USB-Gerät  NFC-Gerät

Um einen USB-Sicherheitsschlüssel zu verwenden, schließen Sie diesen bei Aufforderung an Ihren USB-Port an. Berühren Sie dann den goldenen Kreis oder die Taste (sofern vorhanden), wenn Sie zum Ausführen einer Folgeaktion aufgefordert werden.



Ausführliche Informationen zum Anschließen Ihrer Schlüssel finden Sie auf der Website des Schlüsselherstellers.



Anmeldemethoden verwalten

NAME	ANMELDEMETHODEN	HINZUGEFÜGT AM	ZULETZT VERWENDET	
Yubikey 5	 Sicherheitsschlüssel	25.07.2019 13:40	25.07.2019 13:40	Entfernen

+ [Weiteren Sicherheitsschlüssel hinzufügen](#)

+ [Windows Hello einrichten](#)



Weitere Anwendungsfälle

Use cases:

- 2FA für Bitlocker (PIN + statischer Key)
- Smart Card mit Domänen-Zertifikat + PIN zur Domänen-Anmeldung (wahlweise mit eigener PKI / CA oder öffentlicher CA)
- Authentifizierung / MFA-Absicherung geschäftlicher Cloud Accounts wie z.B. Microsoft Office 365, Azure, AWS, GitHub, Citrix..
- Authentifizierung / MFA-Absicherung privater Cloud Accounts wie z.B. G Suite, Facebook, Dropbox, KeePass, EA Online, Instagram..

(Alle Services siehe > <https://www.yubico.com/works-with-yubikey>)

On-Top-Enforcement: Zero Trust (Conditional Access)



Übersicht

Richtlinien

Insights und Berichterstellung

Diagnose und Problembehandlung

Verwalten

- Benannte Standorte
- Benutzerdefinierte Steuerelemente (Vorschau)
- Nutzungsbedingungen
- VPN-Konnektivität
- Authentifizierungskontexte
- Authentifizierungsstärken
- Klassische Richtlinien

Überwachung

- Anmeldeprotokolle
- Überwachungsprotokolle

Problembehandlung + Support

- Neue Supportanfrage

Phishing-resistente Multi-Faktor-Authentifizierung für Administratoren verlangt

Richtlinie für bedingten Zugriff

Löschen Richtlinieninformationen anzeigen

Steuern Sie den Zugriff basierend auf einer Richtlinie für den bedingten Zugriff, um Signale zusammenzuführen, Entscheidungen zu treffen und Organisationsrichtlinien durchzusetzen. [Weitere Informationen](#)

Name: Phishing-resistente Multi-Faktor-Authentifiz...

Zuweisungen

Benutzer: Bestimmte Benutzer eingeschlossen

Zielressourcen: Alle Ressourcen (früher „Alle Cloud-Apps“)

Netzwerk: NEU Nicht konfiguriert

Bedingungen: 0 Bedingungen ausgewählt

Zugriffskontrollen

Gewähren: 1 Steuerelement ausgewählt

Sitzung: 0 Steuerelemente ausgewählt

Steuern Sie die Zugriffserzwingung, um den Zugriff zu blockieren oder zu gewähren. [Weitere Informationen](#)

Blockzugriff

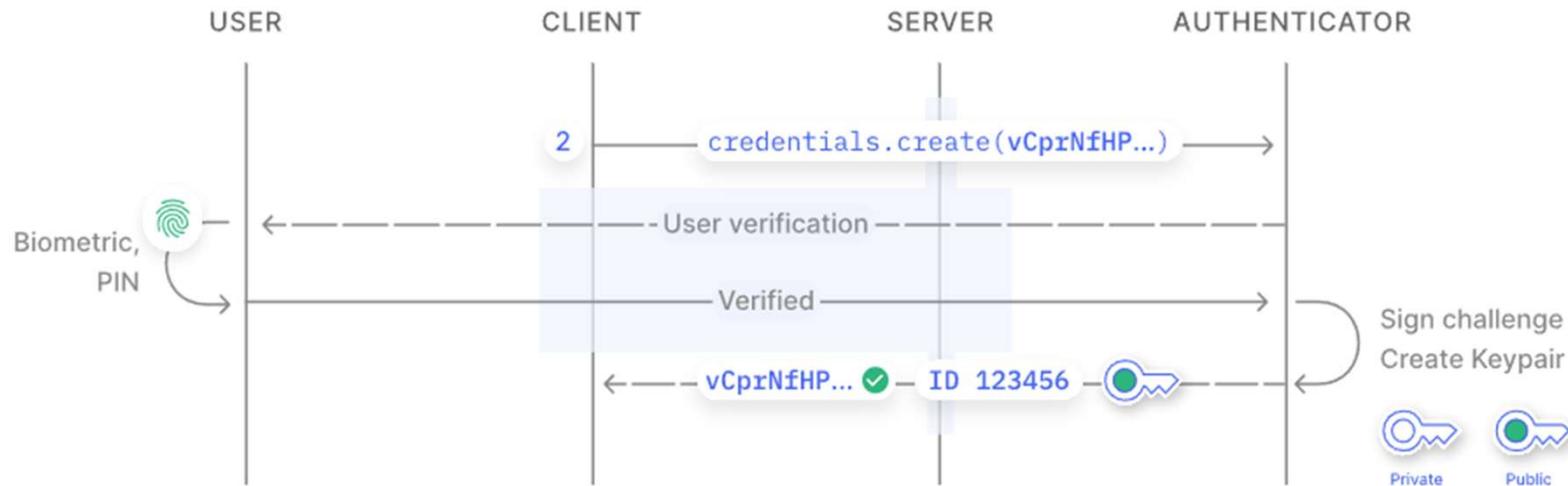
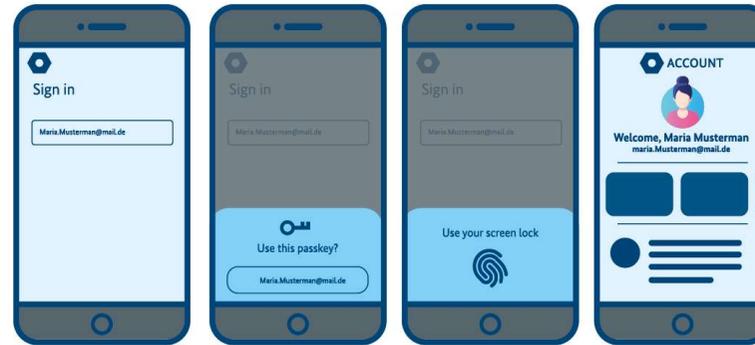
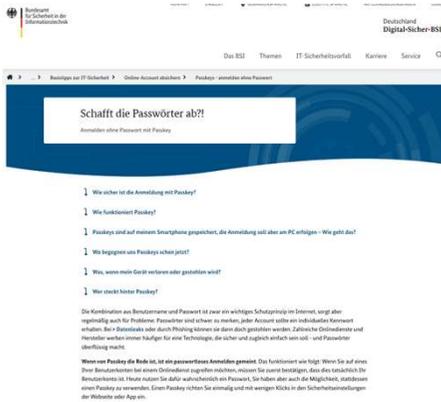
Zugriff gewähren

- Multi-Faktor-Authentifizierung erfordern
- Authentifizierungsstärke erforderlich
Phishing-resistant MFA
- Markieren des Geräts als kompatibel erforderlich
- In Microsoft Entra hybrid eingebundenes Gerät erforderlich
- Genehmigte Client-App erforderlich
[Liste der genehmigten Client-Apps anzeigen](#)
- App-Schutzrichtlinie erforderlich
[Liste der durch Richtlinien geschützten Client-Apps anzeigen](#)
- Kennwortänderung anfordern

Für mehrere Steuerelemente

- Alle ausgewählten Kontrollen anfordern
- Eine der ausgewählten Steuerungen anfordern

„Was ist mit Passkeys auf dem Smartphone?“



„Was ist mit Passkeys auf dem Smartphone?“



Dashlane Synced

Credential ID: cre-12122764971399850491
 Created: 2024-03-25 20:29:31 with Chrome on Android
 Last used: 2024-03-25 20:29:31
 Status: active

NordPass Synced

Credential ID: cre-17138508703930512849
 Created: 2024-03-25 20:27:16 with Chrome on Android
 Last used: 2024-03-25 20:27:16
 Status: active

Passkey

Credential ID: cre-18444682129148227010
 Created: 2023-04-24 13:18:29 with Chrome on Windows
 Last used: 2023-04-24 13:18:29
 Status: active

Passkey Synced

Credential ID: cre-3918235612469588499
 Created: 2024-03-25 20:28:11 with Chrome on Windows
 Last used: 2024-03-25 20:28:12
 Status: active

1Password Synced

Credential ID: cre-4480221369968950588
 Created: 2024-03-25 20:26:05 with Chrome on Android
 Last used: 2024-03-25 20:26:06
 Status: active

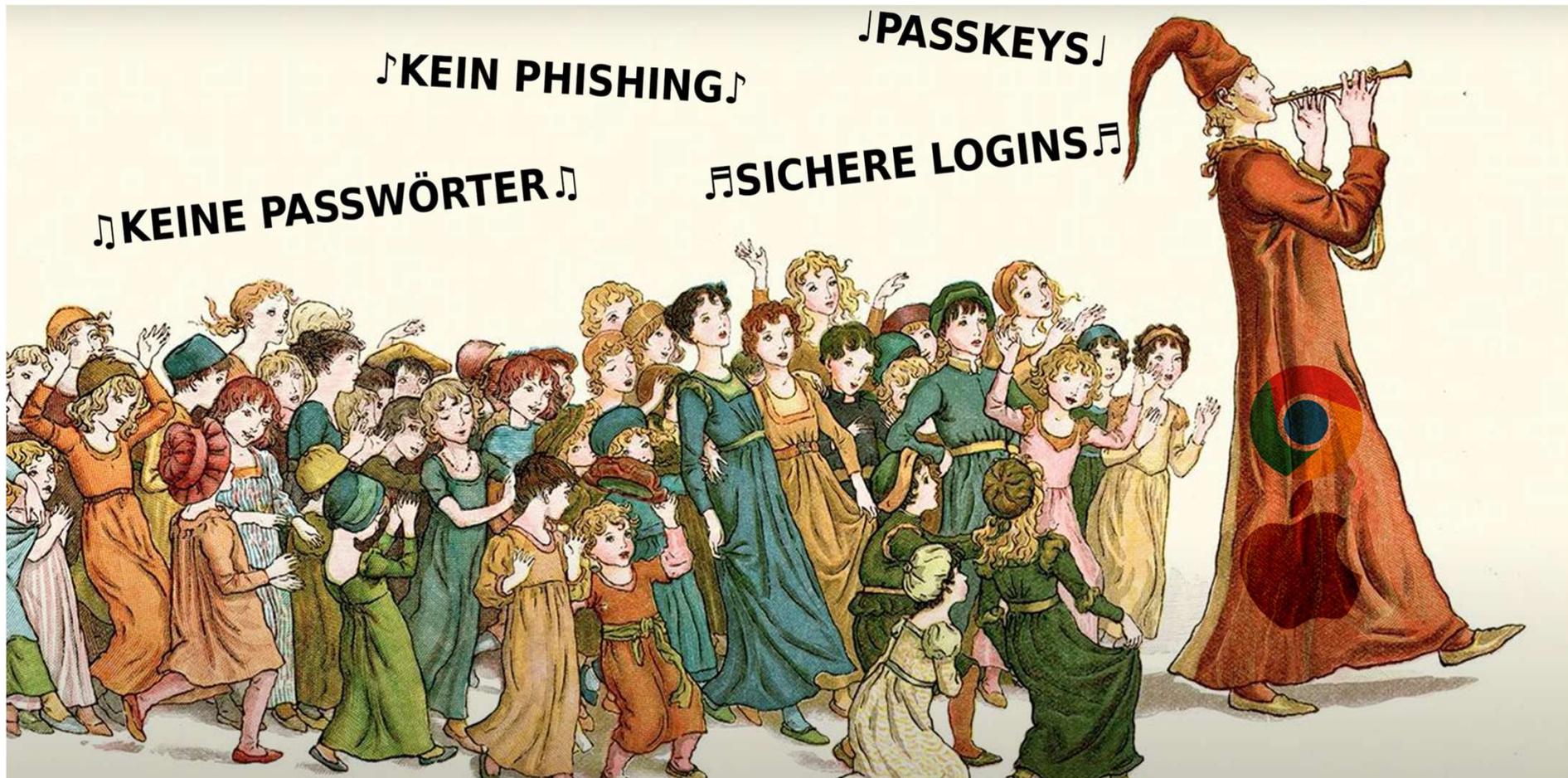
Google Password Manager Synced

Credential ID: cre-6008662616688642260
 Created: 2024-01-23 23:05:34 with Chrome on Android
 Last used: 2024-01-26 17:59:38
 Status: active

[Create a Passkey](#)

	Android 14	iOS 17.4	Web (Windows 11 + Chrome Extension)
First-Party Passkey Provider			
Apple iCloud Keychain	No	Yes	Yes
Google Password Manager	Yes	No	Yes
Windows Hello	No	No	Yes
Third-Party Passkey Provider			
1Password	Yes	Yes	Yes
Bitwarden	No	No?	Yes
Dashlane	Yes	Yes	Yes
Enpass	Yes	Yes	Yes (requires running desktop app in the background)
Keeper	Yes	Yes	Yes
KeePassXC	n/a	n/a	Yes
LastPass	No	No	No
Nordpass	Yes	Yes	Yes
Proton	Yes	Yes	Yes
Samsung Pass	Yes	n/a	n/a (error message)

„Was ist mit Passkeys im Browser?“



„Trau, schau, wem!“



Choosing the right passkey solution

SERVICE PROVIDERS	Consumers	High risk consumers	High value consumers
	Copyable passkeys on their devices are probably okay	Greater security by requiring security keys for passkeys	Differentiate with security keys for passkeys
ENTERPRISES	First line workers	Office workers	Privileged users
	Need a solution that is not dependent on their personal device to authenticate	May require security keys with hardware attestation to know where credentials are stored and meet compliance	Highest risk users – require Security Keys with hardware attestation to know where the credentials are stored.





Unsere Social Media Kanäle

SOCIAL MEDIA KANÄLE DER PEGASUS IT

Auf unseren Social Media Kanälen veröffentlichen wir neueste Informationen zu aktuellen IT-Themen, innovativen Produkten sowie unseren pegasus Events. Zudem erhalten Sie immer wieder Einblicke in unsere Arbeit, Zusammenarbeit mit Partnern und Insights vom Team der pegasus.

Folgen Sie uns auf Facebook, Twitter, Xing & Co und bleiben stets uptodate rund um das Thema IT.



BLUESCREEN – UNSER TECH PODCAST



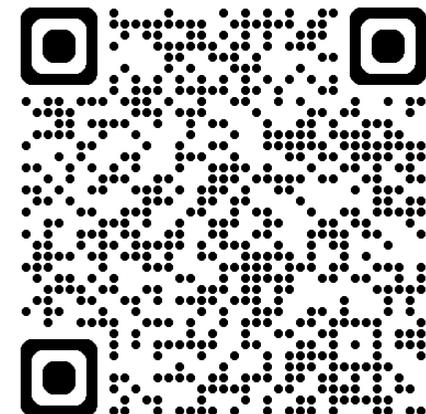
067: Alles über Passkeys! Mit Yvonne Aurich.

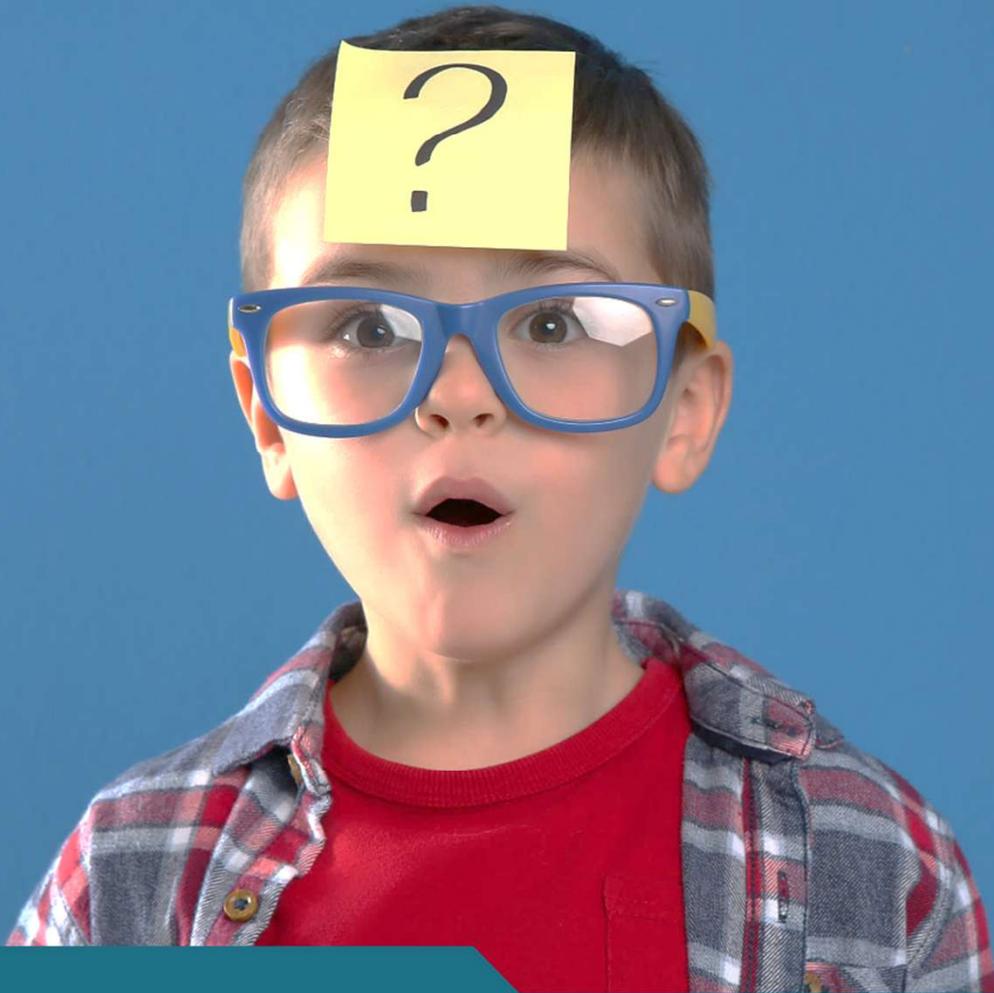
Alle sprechen über Passkeys und deshalb tun wir das heute in diesem Special auch

▶ Episode abspielen 19:34

podigee

Abonnieren Teilen ...





Haben Sie Fragen
oder Anregungen?

pegasus IT – Member of ITVentive Group

ITventive Group

eviatec Systems AG, Monreposstrasse 57, D-71634 Ludwigsburg
pegasus GmbH, Bayernstrasse 10, D-93128 Regenstauf
eviatec Digital Solutions AG, Uferweg 17, CH-3013 Bern
eviatec Scandinavia ApS, Park Alle 295, 2. floor, DK-2605 Brøndby

pegasus-gmbh.de



ITventive® ist eine eingetragene Marke der eviatec Systems AG und der pegasus GmbH in Deutschland und/oder anderen Ländern. eviatec® ist eine eingetragene Marke der eviatec Systems AG in Deutschland und/oder anderen Ländern. Weitere Unternehmens-, Produkt- oder Servicennamen können Marken anderer Hersteller sein.

Diese Veröffentlichung dient nur der unverbindlichen allgemeinen Information und ersetzt nicht die eingehende individuelle Beratung. Die in dieser Veröffentlichung enthaltenen Informationen können jederzeit, auch ohne vorherige Ankündigung, geändert werden. Insbesondere können technische Merkmale und Funktionen auch landesspezifisch variieren. Die Produktinformationen geben den derzeitigen Stand wieder. Gegenstand und Umfang der Leistungen bestimmen sich ausschließlich nach den jeweiligen Verträgen. Die Einhaltung bestimmter Rechtsvorschriften von Produkten und sonstigen Leistungen wird seitens ITventive weder gewährleistet, noch garantiert oder als Eigenschaft zugesichert. Der Kunde ist für die Einhaltung anwendbarer Sicherheitsvorschriften und sonstiger Vorschriften des nationalen und internationalen Rechts verantwortlich.

Änderungen, Irrtümer und Druckfehler bleiben vorbehalten. Nachdruck und Vervielfältigung, auch auszugsweise, nur mit schriftlicher Genehmigung der eviatec Systems AG & pegasus GmbH.

© Copyright eviatec Systems AG & pegasus GmbH 2024. Alle Rechte vorbehalten.