



willkommen



2. Digitale Sprechstunde Gemüinden



Gefördert durch:



Unterstützt von:





Agenda

- 1 Sind noch Fragen zur Veranstaltung vom 14.11.2024
- 2 Heutige Themen
- 3 Ihre Wünsche für die nächste Sprechstunde **???**
- 4 Aktuelle Veränderungen in 2025

Wer die Präsentation(en) per PDF erhalten möchte,
bitte formlose E-Mail an di-bo-westerburg@online.de



Fragen zur letzten Sprechstunde

- Anregungen, Kritik
- Was sollten wir ändern, was verbessern?
- Gerne auch per Mail an di-bo-westerburg@online.de



Ihre offenen Themenwünsche

- E-Mail (Anhänge, ... auf Handy empfangen bzw. senden
- Cyberangriffe, Hackerangriffe, Gefahren im Internet
- Drucken mit dem Handy, Handy mit Drucker verbinden
- ePA für alle – Einführung zum 15.01.2025 **AKTUELL**
- Datenschutz, Datensicherheit, Sicherungskopien erzeugen und einlesen
- Cloudspeicher
- QR-Code
- Datenmüll entfernen, Handy „aufräumen“
- Briefe schreiben – Tipps und Tricks
- Betrugsmaschen, Fakeshops



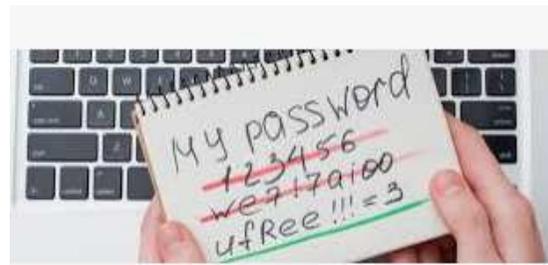
Heutige Themen

Sichere Passworte bilden – die man sich auch merken kann

Router und Telefon administrieren – Bestimmte Nummern blockieren

Handypass – Polizei Köln NRW

Ausblick auf das Jahr 2025 - Änderungen



Ändern Sie **IMMER ALLE** STANDARD-PASSWORTE



Passworthalter



Kriminelle Handlungen

- Internetcafé
- Hotel
- Kur- und Reha-Einrichtungen
- usw.



Wie werden Passworte geknackt???





Key Katcher

Tastaturspion

Alle Tastaturanschläge werden mitgeschrieben

USB Keylogger Wifi



in Aktion



NICHT LUSTIG!

- Ein Keylogger kann sich aber auch als Virus auf dem Computer befinden!!!



5 Warnsignale für Keylogger

- Unbekannte laufende Prozesse und Einträge im Task Manager
- Auffällige Einträge im Aktivitätenprotokoll eurer Firewall
- Langsamer Browser
- Verzögerte Mausbewegungen und Tastatureingaben
- Verschwindender Cursor



Welche Strategien nutzen Hacker um ein Passwort zu knacken?



- **Sichten** Zettel, Passworthalter usw.
- **Probieren** händische Eingaben „häufig verwendete PW“ oder persönliche Daten, Hobbies, Freizeit, Familie
- **Buchstaben** händisch oder mit SW-Programmen „Buchstabenfolgen“
- **Wörter** SW-Programmen „Wörter und Wort-Zahl-Kombinationen“

Es können mehrere Wörterbücher in wenigen Minuten ausprobiert werden

Passwort-Listen zum Download

 GitHub
<https://github.com> > Passwords · [Diese Seite übersetzen](#) ⋮
10-million-password-list-top-1000000.txt
10-million-password-list-top-1000000.txt ...

 GitHub
<https://github.com> > Passwords > Common-Credentials ⋮
10-million-password-list-top-10000.txt
123456 password 12345678 qwerty 123456789 12345 1234 111111 1234567 dragon 123123
baseball abc123 football monkey letmein 696969 shadow master 666666 ...

 Kaggle
<https://www.kaggle.com> > wjburns · [Diese Seite übersetzen](#) ⋮
Common Password List (rockyou.txt)
rockyou.txt contains 14,341,564 unique passwords, used in 32,603,388 accounts. Kali Linux
provides this dictionary file as part of its standard installation.

 Kaggle
<https://www.kaggle.com> > code · [Diese Seite übersetzen](#) ⋮
Common Password List (rockyou.txt)
Common **Password List (rockyou.txt)**. Built-in Kali Linux wordlist rockyou.txt. Cover image.
arrow_drop_up 603. file_downloadDownload (53 MB)

 freeCodeCamp
<https://www.freecodecamp.org> > ... · [Diese Seite übersetzen](#) ⋮
How to Crack Passwords using John The Ripper
17.11.2022 — Here is a common **password list called rockyou.txt**. While you can use popular
wordlists like RockYou, John also has its own set of wordlists ...



Sicheres Passwort

- Jede(r) benötigt ein sicheres Passwort
- Für **jede** Anwendung ein **anderes** Passwort
 - E-Mail, Benutzerkonten, Online Banking, Foren, Kundenportale usw.
- **Jedes Passwort kann geknackt werden**
- Entscheidend ist aber die **Zeit**, die dafür benötigt wird

Sicheres Passwort

Passwortlänge	68 unterschiedliche Zeichen	94 unterschiedliche Zeichen
1	8,5 Mikrosekunden	11,75 Mikrosekunden
2	0,58 Millisekunden	1,10 Millisekunden
3	0,39 Sekunden	0,90 Sekunden
4	2,67 Sekunden	9,76 Sekunden
5	3,03 Minuten	15,29 Minuten
6	3,43 Stunden	23,95 Stunden
7	9,73 Tage	93,82 Tage
8	1,81 Jahre	24,14 Jahre
9	123,14 Jahre	2260 Jahre
10	8370 Jahre	213350 Jahre
11	569380 Jahre	10,05 Millionen Jahre
12	38,72 Millionen Jahre	1,89 Milliarden Jahre

Sicheres Passwort

Passwortlänge	68 unterschiedliche Zeichen	94 unterschiedliche Zeichen
1	8,5 Mikrosekunden	11,75 Mikrosekunden
2	0,58 Millisekunden	1,10 Millisekunden
3	0,39 Sekunden	0,90 Sekunden
4	2,67 Sekunden	9,76 Sekunden
5	3,03 Minuten	15,29 Minuten
6	3,43 Stunden	23,95 Stunden
7	9,73 Tage	93,82 Tage
8	1,81 Jahre	24,14 Jahre
9	123,14 Jahre	2260 Jahre
10	8370 Jahre	213350 Jahre
11	569380 Jahre	10,05 Millionen Jahre
12	38,72 Millionen Jahre	1,89 Milliarden Jahre

Sicheres Passwort

Passwortlänge (Zeichen)	nur Zahlen	nur Kleinbuchstaben	Klein- & Großbuchstaben	Zahlen und Klein- /Großbuchstabe n	Zahlen Klein- /Großbuch- staben, und Symbole
4	Sofort	Sofort	3 Sekunden	6 Sekunden	9 Sekunden
5	Sofort	4 Sekunden	2 Minuten	6 Minuten	10 Minuten
6	Sofort	2 Minuten	2 Stunden	6 Stunden	12 Stunden
7	4 Sekunden	50 Minuten	4 Tage	2 Wochen	1 Monat
8	37 Sekunden	22 Stunden	8 Monate	3 Jahre	7 Jahre
9	6 Minuten	3 Wochen	33 Jahre	161 Jahre	479 Jahre
10	1 Stunde	2 Jahre	1 Tsd. Jahre	9 Tsd. Jahre	33 Tsd. Jahre
11	10 Stunden	44 Jahre	89 Tsd. Jahre	618 Tsd. Jahre	2 Mio. Jahre
12	4 Tage	1 Tsd. Jahre	4 Mio. Jahre	38 Mio. Jahre	164 Mio. Jahre
13	1 Monat	29 Tsd. Jahre	241 Mio. Jahre	2 Mrd. Jahre	11 Mrd. Jahre
14	1 Jahr	766 Tsd. Jahre	12 Mrd. Jahre	147 Mrd. Jahre	805 Mrd. Jahre
15	12 Jahre	19 Mio. Jahre	652 Mrd. Jahre	9 Bio. Jahre	56 Bio. Jahre
16	119 Jahre	517 Mio. Jahre	33 Bio. Jahre	566 Bio. Jahre	3 Brd. Jahre
17	1 Tsd. Jahre	13 Mrd. Jahre	1 Brd. Jahre	35 Brd. Jahre	276 Brd. Jahre
18	11 Tsd. Jahre	350 Mrd. Jahre	91 Brd. Jahre	2qn Trill. Jahre	19qn Trill. Jahre



Sichere Passwörter

Generell gilt

- ✓ Ein individuelles Passwort pro Account!
- ✓ Eine Mehr-Faktor-Authentisierung (ergänzend zum Passwort durch bspw. eine Gesichtserkennung, eine App-Bestätigung, E-Mail oder einer PIN auf einem anderen Gerät) ist empfehlenswert.
- ✓ Alle verfügbaren Zeichen nutzen inklusive Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen (Leerzeichen, ?!%+...).
- ✓ Das vollständige Passwort sollte nicht im Wörterbuch vorkommen.

Zu vermeiden

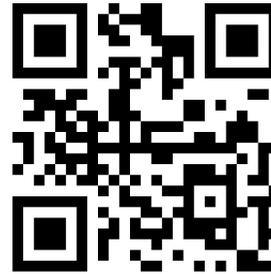
- ✗ Namen von Familienmitgliedern, Haustieren, Geburtsdaten etc.
- ✗ Einfache oder bekannte Wiederholungs- bzw. Tastaturmuster wie „asdfgh“ oder „1234abcd“
- ✗ Ziffern oder Sonderzeichen an den Anfang oder ans Ende eines ansonsten einfachen Passwortes.
- ✗ Dasselbe Passwort bei mehr als einem Account.



Sichere Passwörter



🔒 checkdeinpasswort.de



Digital Botschafterinnen
& Botschafter
Rheinland-Pfalz

WIE SICHER IST MEIN PASSWORT?

Probiere verschiedene Passwörter aus!

⚠️ Aus Sicherheitsgründen solltest du nicht deine echten Passwörter eingeben.



haveibeenpwned.com



Digital Botschafterinnen
& Botschafter
Rheinland-Pfalz

';--wurde ich gehackt?

Überprüfen Sie, ob Ihre E-Mail-Adresse von einem Datenschutzverstoß betroffen ist

E-Mail-Adresse oder Handynummer eingeben

pwniert?

Die Nutzung von Have I Been Pwned unterliegt [den Nutzungsbedingungen](#)

Wie bilde ich ein sicheres Passwort?

- Ersetzen-Trick Leetspeak „eigener Code“
- Buchstaben durch Sonderzeichen und Zahlen ersetzt
 - Passwortsicherheit
 - Pa\$sw0rts/ch3rhe1t
- Wer möchte, kann auch sog. Leetspeak-Übersetzer nutzen

 Toolpage
<https://de.toolpage.org/tool/leetspeak> ⋮
Leetspeak-Übersetzer

 dCode
<https://www.dcode.fr/leet-speak> · Diese Seite übersetzen ⋮
Leet Speak Translator - 1337 - Online Leetspeak Decoder, ...

Wie bilde ich ein sicheres Passwort?

- **Satz-Trick**
- Denken Sie sich einen Satz aus, nehmen Sie nun nur die Anfangsbuchstaben, Zahlen und Sonderzeichen
- Heute Nachmittag gehe ich mit Johanna um 15:30 Uhr einen Kaffee trinken.

• **HNgimJu15:30UeKt§**

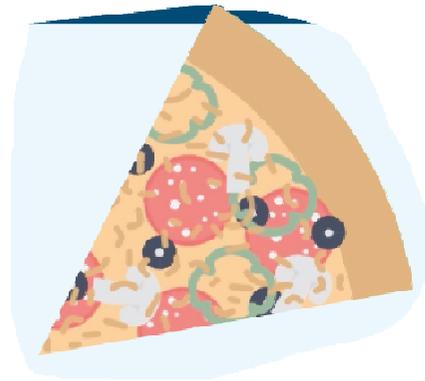
Wie bilde ich ein sicheres Passwort?

- **Satz-Trick** **Beispiele**
- **Mit 66 Jahren, da fängt das Leben an...**
- **Atemlos durch die Nacht, ...**
- **Was Hänschen nicht lernt, ...**
- **Ich war noch niemals in New York ...**
- **Weltersburg, ein schöner Ort, hier will ich nicht mehr fort**

Wie bilde ich ein sicheres Passwort?

Was hat Ihr Passwort mit Pizza zu tun?

Denken Sie sich einen Satz aus, der mindestens eine Zahl enthält, zum Beispiel:



„**A**m liebsten **e**ссе ich **P**izza
mit **4** Zutat**e**n und **e**xtra **K**äse!“

Merken Sie sich nun den ersten Buchstaben eines jeden Wortes und Sie erhalten ein starkes und sicheres Passwort.

AeiPm4Z+eK!



Wie bilde ich ein sicheres Passwort?

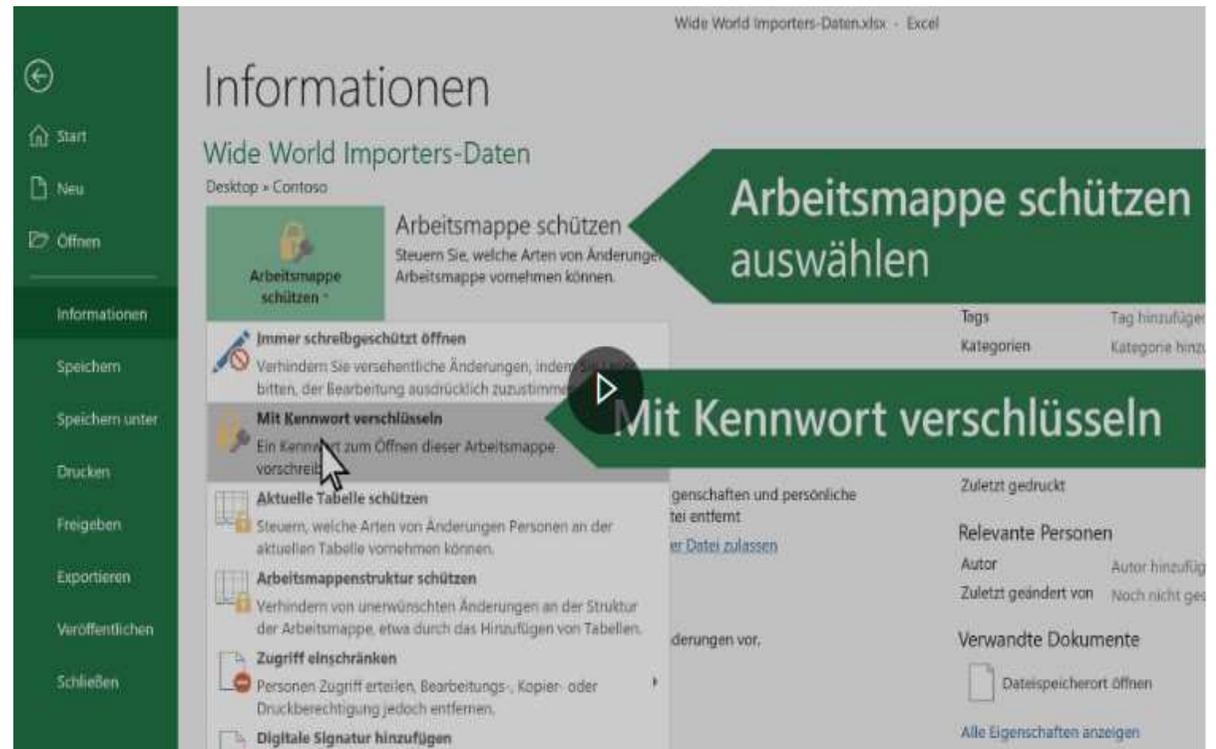
- Wort-Trick
- **Aneinanderreihung von Wörtern** (ohne Sinnzusammenhang)
- Handball – Wahlparty – Rentnerdasein + „Sonderzeichen“
- **HandballWahlpartyRentnerdasein§%\$**

Wie bilde ich sichere Passworte

- Passwort **variieren**
- **NIE** überall das gleiche Passwort verwenden
- **Zu dem sicheren Passwort einfach am Anfang oder am Ende eine bestimmte Anzahl von Buchstaben ergänzen und somit die betreffende Anwendung vermerken**
- **HNgimJu15:30UeKt§** **Basispasswort**
- **EM_HNgimJu15:30UeKt§** **(für E-Mail)**
- **AZ_HNgimJu15:30UeKt§** **(für Amazon)**
- **EB_HNgimJu15:30UeKt§** **(für ebay)**

MS Excel – Datei mit Kennwort schützen

1. Wählen Sie **Datei** > **Informationen** aus.
2. Wählen Sie das Feld **Arbeitsmappe schützen** und dann **Mit Kennwort verschlüsseln** aus.
3. Geben Sie im Feld **Kennwort** ein Kennwort ein, und wählen Sie **OK** aus.
4. Bestätigen Sie das Kennwort im Feld **Kennwort erneut eingeben**, und wählen Sie **OK** aus.



Passwortmanager

Passwortmanager 7/2022



1Password



AceBit Password Depot 16



Avira Password Manager (Pro)



Bitwarden Premium



Dashlane Premium



Enpass Individual Plan



F-Secure ID Protection



Kaspersky Password Manager
(Premium)



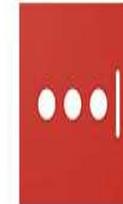
KeePassXC



Keeper Security Keeper Unlimited



Lamantine Software Sticky
Password (Premium)



LastPass Premium



McAfee True Key (Premium)



Nord Security NordPass (Premium)



SafelInCloud Individual Pro



Siber Systems RoboForm
(Everywhere)



2-Faktor-Authentifizierung / Authentisierung

- Kurzform: **2FA**
- Es gibt unterschiedliche Varianten
- Im Online Banking ist es **verpflichtend**
- WISSEN + MERKMAL (Biometrie) / Besitz



"What too much is, is too much",
"Was zuviel ist, ist zuviel"

SIE HABEN PROBLEME MIT
MATHEMATIK
RUFEN SIE UNS AN

24 Stunden Notdienst  7 Tage die Woche

0180
[21²x6Y]+46:19%-(4711+3³)





Heutige Themen

Sichere Passworte bilden – die man sich auch merken kann

Router und Telefon administrieren – Bestimmte Nummern blockieren

Handypass – Polizei Köln NRW

Ausblick auf das Jahr 2025 - Änderungen





- 1 Neuen Kontakt anlegen Mister Nervig
- 2 Telefonnummer +49 176 81828384
- 3 Diese Nummer blockieren
- 4 Diese Blockierung aufheben



Nummern blockieren

1. Öffnen Sie die Telefon App .
2. Tippen Sie auf das Dreipunkt-Menü Anrufliste .
3. Tippen Sie auf einen Anruf von der Nummer, die **blockiert** werden soll.
4. Tippen Sie auf **Blockieren**/Spam melden.



Rufnummern, Kontakte und E-Mail-Adressen auf dem iPhone oder iPad blockieren

Es gibt verschiedene Möglichkeiten, wie du Rufnummern, Kontakte und E-Mail-Adressen blockieren kannst.

Telefon

Tippe in der Telefon-App auf „Anrufliste“, und tippe dann auf die Infotaste ⓘ neben der Telefonnummer oder dem Kontakt, den du blockieren möchtest. Scrolle nach unten, und tippe anschließend auf „Anrufer blockieren“.

Nachrichten

Öffne in der Nachrichten-App die entsprechende Konversation, und tippe auf den Kontakt oben in der Konversation. Tippe auf die Info-Taste ⓘ, scrolle nach unten, und tippe dann auf „Anrufer blockieren“.

Du kannst eine Telefonnummer oder E-Mail-Adresse auch direkt in der Einstellungen-App zur Liste „Blockierte Kontakte“ hinzufügen.

FaceTime

Tippe in der FaceTime-App auf die Infotaste ⓘ neben der Telefonnummer, dem Kontakt oder der E-Mail-Adresse, die du blockieren möchtest. Scrolle nach unten, und tippe anschließend auf „Anrufer blockieren“.

Mail

Öffne in der Mail-App die E-Mail mit dem Kontakt, den du blockieren möchtest, und tippe dann oben auf den Kontakt. Tippe auf „Diesen Kontakt blockieren“.

- Die Benutzeroberfläche können Sie entweder über <http://fritz.box> oder die IP-Adresse der FRITZ!Box (in den Werkseinstellungen <http://192.168.178.1>) aufrufen. Ausserdem ist die FRITZ!Box immer über die Notfall-IP <http://169.254.1.1> erreichbar.



Geben Sie in die Adresszeile Ihres Browsers Folgendes ein:
<http://speedport.ip> oder <http://192.168.2.1> (bei Funkroutern:
<http://192.168.1.1>). Bestätigen Sie die Eingabe mit "Enter". Es öffnet sich
die Anmeldeseite.





Heutige Themen

Sichere Passworte bilden – die man sich auch merken kann

Router und Telefon administrieren – Bestimmte Nummern blockieren

Handypass – Polizei Köln NRW

Ausblick auf das Jahr 2025 - Änderungen



Handy weg, was nun? Präventionstipps der Polizei zum Thema Raub, Diebstahl oder sonstigem Verlust

www.lka.polizei.nrw.de

- > Informieren Sie sich bei Ihrem Anbieter über die Möglichkeit einer IMEI-Sperre.
- > Nutzen Sie die Handy-Funktion einiger Hersteller, wie z.B. „Info über SIM-Wechsel“. Damit können Sie sich z.B. die neue SIM-Kartennummer des Täters zusenden und der Polizei zukommen lassen.

Herausgeber:
Landeskriminalamt Nordrhein-Westfalen
Völklinger Straße 49
40221 Düsseldorf

Telefon: 0211 939-0
Telefax: 0211 939-3229
E-Mail: poststelle.lka@polizei.nrw.de
Internet: www.lka.polizei.nrw.de

Ansprechpartner:
Landeskriminalamt NRW
Abteilung 3
Dezernat 32
Sachgebiet 32.2 – Technische Prävention,
Prävention von Vermögens- und
Eigentumsdelikten

Telefon: 0211 939-3205
Telefax: 0211 939-3229
E-Mail: einbruchschutz@polizei.nrw.de

Stand: Februar 2017

Bildnachweis:
© Scanrail / fotolia.com

Handypass

Dieser Handypass enthält die wichtigsten Verhaltenstipps beim Verlust Ihres Handys/Smartphones. Auf der Rückseite haben Sie die Möglichkeit die wesentlichen Informationen für den Notfall einzutragen.

ausfüllen, abtrennen und einstecken

Handypass

Rufnummer:

IMEI-Nummer:

SIM-Karte:

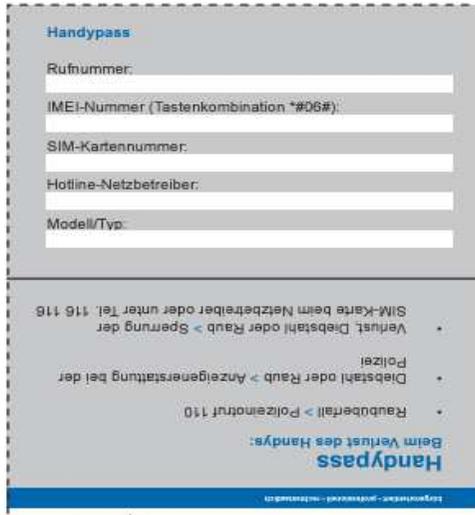
Hotline-Netzbetreiber:

Modell/Typ:



Handypass Zum Selbstdruck

- Handypass ausdrucken
- an der gestrichelten Linie ausschneiden
- Handypass ausfüllen und an der schwarzen Linie falten



Handypass

Rufnummer: _____

IMEI-Nummer (Tastenkombination *#06#): _____

SIM-Kartennummer: _____

Hotline-Netzbetreiber: _____

Modell/Typ: _____

Beim Verlust des Handys:
Handypass

- Raubüberfall > Polizeinotruf 110
- Diebstahl oder Raub > Anzeigenerstattung bei der Polizei
- Verlust, Diebstahl oder Raub > Sperrung der SIM-Karte beim Netzbetreiber oder unter Tel. 116 116



Handypass

Rufnummer: _____

IMEI-Nummer (Tastenkombination *#06#): _____

SIM-Kartennummer: _____

Hotline-Netzbetreiber: _____

Modell/Typ: _____

Beim Verlust des Handys:
Handypass

- Raubüberfall > Polizeinotruf 110
- Diebstahl oder Raub > Anzeigenerstattung bei der Polizei
- Verlust, Diebstahl oder Raub > Sperrung der SIM-Karte beim Netzbetreiber oder unter Tel. 116 116





Heutige Themen

Sichere Passworte bilden – die man sich auch merken kann

Router und Telefon administrieren – Bestimmte Nummern blockieren

Handypass – Polizei Köln NRW

Ausblick auf das Jahr 2025 - Änderungen

25.05.2023 Infoveranstaltung in Willmenrod



Digital Botschafterinnen
& Botschafer
Rheinland-Pfalz

„Wir sind bereit Ihnen zu helfen!“



Digital aktive Senioren

Der Digitalbotschafter der Verbandsgemeinde, Michael Roth und Ortsbürgermeister Günter Weigel zeigten sich sehr zufrieden mit der Auftaktveranstaltung zur digitalen Teilhabe der Gruppe Ü65 in Willmenrod. Zusammen mit Ute Held vom Kirchenvorstand der evangelischen Gemeinde in Willmenrod konnten beide 18 Gäste begrüßen, die sich die Möglichkeiten der Digitalbotschafter erklären ließen. Im Kern geht es darum auf ehrenamtlicher Basis die mannigfachen Möglichkeiten der Digitalisierung für jeden einzelnen auch im Alter zu erfahren, aber auch auf die Gefahren hinzuweisen. Zudem betonte der Ortsbürgermeister, gehe es auch darum, mit diesen thematischen Veranstaltungen den sozialen Aspekt des Dorftreffs ein Stück weit wiederzubeleben, der in der Corona-Zeit leider eingestellt werden musste.



Im Anschluss an den Vortrag wurde ein erster Arbeitskreis gebildet. Jeden ersten Mittwoch im Monat ab 18 Uhr soll im Martin-Luther-Haus zunächst eine Sprechstunde für direkte persönliche Fragen in Sachen Handy, Tablet und PC stattfinden. Anschließend geht es dann mit einem Thema weiter. Beim nächsten Treff am Mittwoch, den 7. 6. geht es nach der Sprechstunde um Online-Banking und die verschiedenen Möglichkeiten und Risiken digitalen Geldverkehrs.

04.12.2024, 17. Digitale Sprechstunde in Willmenrod



Digital Botschafterinnen
& Botschafer
Rheinland-Pfalz



**Wir geben
alles,
nur nicht
auf!**





Wir müssen unser Angebot stark einschränken



- Auf „Anfängerthemen“ und direkte Hilfe beschränken
- Feste Beratungstage in der VG Westerburg in Planung
- Telefonische Sprechstunden anbieten
- Die gerade erst gestarteten Sprechstunden gehen weiter und können gerne besucht werden
(Bellingen, Weltersburg, Gemünden)



- Erneuter Aufruf im Wochenspiegel DiBo in 2025
- Unterstützung aus Mainz wird bereits gesucht
- Zusammenarbeit mit VHS aus anderen Gemeinden
- Wir suchen sehr aktiv nach neuen Lösungen mit der Verbandsgemeinde Westerburg
- Informationen erfolgen über den Wäller Wochenspiegel



Kontaktmöglichkeiten

- Michael Roth



di-bo-westerburg@online.de



02663-9649942



- Weitere Kontakte und Informationen gibt es auf der Webseite <https://digital-botschafter.Cyberangriffe/>
(„Veranstaltungen“ – werden alle aktuellen Termine angezeigt)
- Mitteilungen im Wäller Wochenspiegel beachten
- Wir kontaktieren Sie gerne per E-Mail zu Veranstaltungen



Ihre Themenwünsche für **09.01.2025**

Themenwünsche:

PC – Administration – Benutzer, Kennwörter, Berechtigungen usw.

ePA für alle – Einführung der elektronischen Patientenakte



Zeit für Ihre Fragen



Gute Fahrt – schönen Abend noch!



Digital Botschafterinnen
& Botschafter
Rheinland-Pfalz



Wir wünschen Ihnen alles Gute!!!

