



DIGITALE

**WEITERENTWICKLUNG
FÜR ALLE**

Gefördert durch das Bayerische Staatsministerium für Unterricht und Kultus.

Bayerisches Staatsministerium für
Unterricht und Kultus



Digitale Sicherheit

Ebersberg, 17.03.2026

Digitale Sicherheit

1. Technische Sicherheit

- **Aktualisierung der Software (Updates)**
- **Passwörter**
- **Datensicherungen (Backups)**
- **Virenerkennung**

2. Sicheres Verhalten

- Abgreifen von Zugangsdaten – „Phishing“
- Betrugsversuche – „Scam“
- Soziale Netzwerke

Aktualisierungen der Software (Updates)

Nutzer zögern Updates oft hinaus, weil sie befürchten, dass nach dem Update etwas nicht mehr (wie gewohnt) funktioniert.

Aber:

Updates beheben Schwachstellen und Fehler in Programmen, und viele „Hackerangriffe“ nutzen solche Schwachstellen und Fehler aus.

Aktualisierungen der Software – jeder Software

Es genügt nicht, wenn man regelmäßig sein Betriebssystem aktualisiert (z.B. Windows Updates).

Alle (!) installierten Programme müssen regelmäßig aktualisiert werden.

Wenn ein Programm „automatische Updates“ anbietet, dann sollte man das unbedingt nutzen!

Programme, die das nicht anbieten, müssen von Hand aktualisiert werden.

Digitale Sicherheit

Aktualisierungen der Software – jedes Geräts

- PCs / MACs
- Handys
- Tablets
- Router
- WLAN-Repeater (Verstärker für das WLAN-Signal)
- „smarte“ Fernseher
- „smarte“ Lautsprecher
- ...jedes Gerät, das mit dem heimischen Netzwerk oder WLAN verbunden wurde!

Aktualisierungen der Software – digitale Hygiene

- **Wird ein Programm nicht mehr verwendet, sollte es deinstalliert werden.**
- **Wird ein Gerät nicht mehr verwendet, sollte es vom Netzwerk getrennt werden (und „zurückgesetzt“ werden, damit keine persönlichen Daten mehr auf dem Gerät sind).**

Digitale Sicherheit

Passwörter

Gute Passwörter erfüllen folgende Eigenschaften:

- **Geheim!**
- **Lang!**
- **Einmalig!**

Digitale Sicherheit

Passwörter: Geheim!

- **Nichts, was im Wörterbuch steht!**
z.B. „Ägypten“
- **Nichts, was man herausfinden kann:**
z.B. Namen und Geburtstage von Angehörigen
- **Niemandem verraten!**

Digitale Sicherheit

Passwörter: Lang!

- **Mindestens 12 Zeichen!**
- **Möglichst viele Zeichenarten: Groß- und Kleinbuchstaben, Ziffern, Sonderzeichen!**

Digitale Sicherheit

Passwörter: Lang!

Mathematik:

- **12 Kleinbuchstaben**
ca. 95.000.000.000.000.000 Möglichkeiten
- **12 beliebige Zeichen**
ca. 19.000.000.000.000.000.000.000 Möglichkeiten

Digitale Sicherheit

Passwörter: Einmalig!

- **Für jeden Dienst ein anderes Passwort verwenden!**
- **Werden bei einem Dienst Zugangsdaten „gestohlen“, versuchen die Datendiebe diese auch bei anderen Diensten zu verwenden.**

Digitale Sicherheit

„Gute“ Passwörter:

Kryptisch (viele Zeichentypen):

„QkadV+A5zGjMSL“

Besonders lang (aber weniger Zeichentypen):

„November Florenz Hotel Ausstellung Kunst“

Digitale Sicherheit

„Gute“ Passwörter:

„November Florenz Hotel Ausstellung Kunst“

- **Jedes der Wörter steht – für sich – im Wörterbuch.**
- **Die persönliche Kombination aber nicht!**

ca. 24.300.000.000.000.000.000.000.000 Möglichkeiten

Digitale Sicherheit

„Gute“ Passwörter:

Beispiel, aus einem Satz gebildet:

„Abends putze ich mir drei Minuten lang die Zähne und gehe dann ins Bett.“

→ „ApimdMldZugd1B“

Ziffern und Sonderzeichen statt mancher Buchstaben:

→ „Ap1m3M!dZugd1B“

Wichtig: Selbst ausdenken, keine Zitate verwenden!

Passwörter merken?

...meist unmöglich!

Lösung: „Passwort Manager“

Zum Beispiel „KeePass“ (kostenlos), „Roboform“ oder „1Password“

Einige Virens Scanner-Pakete enthalten auch einen Passwort Manager.

Passwörter sind trotzdem knackbar!

Lösung: 2-Faktor-Anmeldung

Wenn das angeboten wird, sollte es genutzt werden, z.B.:

- **Code per SMS**
- **Authenticator-App auf dem Smartphone**
- **Hardware-Schlüssel (z.B. Yubikey)**

Teilweise aufwändiger in der Einrichtung und Verwendung!

Passwörter sind trotzdem knackbar!

Lösung: Passkeys

Muss ebenfalls vom jeweiligen Dienst unterstützt werden!

Passkey wird auf dem Smartphone/Tablet/Laptop/PC abgelegt.

=> Bei Defekt benötigt man einen zweiten Zugangsweg!

Passwörter: Tipps vom BSI

Sichere Passwörter erstellen:

<https://www.bsi.bund.de/dok/6596574>

Passwörter merken:

<https://www.bsi.bund.de/dok/6701116>

Datensicherungen (Backups)

Jedes Speichermedium in Computern, Handys, Tablets, etc. geht irgendwann kaputt!

...meist ohne Vorwarnung.

Alle Daten, die sich nur auf diesem Speichermedium befinden, sind dann verloren.

Datensicherungen (Backups)

Kopien auf demselben Gerät sind keine Datensicherung!

Besser:

- **externe Speicher (z.B. USB-Sticks, USB-Festplatten)**
- **Netzlaufwerke („NAS“)**
- **vertrauenswürdiger (!) Cloud-Speicher**

Datensicherungen (Backups) – 3-2-1-Regel

- **mindestens 3 Kopien aller wichtigen Daten**
- **auf 2 verschiedene Speichermedien**
- **davon 1 Kopie außer Haus**

Datensicherungen (Backups)

Keine wichtigen Daten vergessen:

- **Passwörter des Passwort Managers**
- **E-Mails und Einstellungen des Mailprogramms (z.B. MOBackup für Outlook)**
- **Einstellungen und Lesezeichen des Internet Browsers**
- **Lizenzschlüssel für Software**
- **Dokumente, Fotos, ...**

Virenerkennung

Ein solider Virens Scanner ist bei Windows 10 und 11 bereits enthalten (Microsoft Defender).

Kaufliche Virens Scanner sind i.d.R. nicht besser, bringen aber Zusatzfunktionen mit (z.B. Suche nach Updates, Passwort Manager).

Digitale Sicherheit

Virenerkennung

Bitte nur einen Virens Scanner einsetzen!

Mehrere können den Computer bremsen und sich sogar gegenseitig stören.

Virenerkennung

Ein Virens Scanner... ist kein Virenschutz!

- **Programme nur aus sicheren Quellen installieren!**
- **Nicht auf E-Mails oder Webseiten hereinfallen, die angebliche Vireninfektionen anzeigen!**

Digitale Sicherheit

1. Technische Sicherheit

- Aktualisierung der Software (Updates)
- Passwörter
- Datensicherungen (Backups)
- Virenerkennung

2. Sicheres Verhalten

- Abgreifen von Zugangsdaten – „Phishing“
- Betrugsversuche – „Scam“ und „Scareware“
- Soziale Netzwerke

Abgreifen von Zugangsdaten („Phishing“)

- **meist per E-Mail, Messenger (z.B. WhatsApp) oder SMS**
- **meist unpersönliche Anrede**
- **angeblich dringend**
- **oft ungenaue/fehlerhafte Formulierungen**



Willkommen zur Registrierung für Mastercard® Identity Check™

Sehr geehrte Damen und Herren,

Mastercard® Identity Check™ ist ein von Mastercard® entwickelter Sicherheitsstandard für Kreditkartenzahlungen, der darauf abzielt, das Risiko von Kartenmissbrauch deutlich zu minimieren.

Ab sofort müssen nahezu alle Online-Zahlungen nach Eingabe Ihrer Kartendetails durch die zusätzliche Bestätigung. Dies gewährleistet einen zusätzlichen Schutz vor unbefugter Nutzung Ihrer Kreditkarte. Dieses Verfahren steht für eine sichere Transaktion auf beiden Seiten.

die Möglichkeiten der 2-Faktor-Authentifizierung eine zusätzliche Sicherheitsebene und damit vollstes Vertrauen.

Aktivieren Sie Ihre Karte Lufthansa Miles & More Credit Card für Mastercard® Identity Check™, um sie beim Online-Einkaufen zu aktivieren. Sie sich jetzt.

Für Mastercard® Identity Check™ können Sie sich kostenlos und schnell registrieren. Klicken Sie auf den folgenden Link, um Aktivieren:

- [→ Jetzt Aktivieren Mastercard® Identity Check™](#)

Beachten Sie: Bei fehlender Registrierung wird die Internetzahlung nicht durchgeführt. Eine Registrierung während des Bezahlvorgangs ist erforderlich.



Willkommen zur Registrierung für Mastercard® Identity Check™

Sehr geehrte Damen und Herren,

Mastercard® Identity Check™ ist ein von Mastercard® entwickelter Sicherheitsstandard für Kreditkartenzahlungen, der darauf abzielt, das Risiko von Kartenmissbrauch deutlich zu minimieren.

Ab sofort müssen nahezu alle Online-Zahlungen nach Eingabe Ihrer Kartendetails durch die zusätzliche Bestätigung. Dies gewährleistet einen zusätzlichen Schutz vor unbefugter Nutzung Ihrer Kreditkarte. Dieses Verfahren steht für eine sichere Transaktion auf beiden Seiten.

die Möglichkeiten der 2-Faktor-Authentifizierung eine zusätzliche Sicherheitsebene und damit vollstes Vertrauen.

Aktivieren Sie Ihre Karte Lufthansa Miles & More Credit Card für Mastercard® Identity Check™, um sie beim Online-Sie sich jetzt.

Für Mastercard® Identity Check™ können Sie sich kostenlos und schnell registrieren.

Klicken Sie auf den folgenden Link, um Aktivieren:

• [→ Jetzt Aktivieren Mastercard® Identity Check™](#)

Beachten Sie: Bei fehlender Registrierung wird die Internetzahlung nicht durchgeführt. Eine Registrierung während des Bezahlvorga

Ihre Finanz-Nachrichten für den Dezember.

Sehr geehrter Kunde,

Wir möchten Sie nochmals daran erinnern, Ihre ING App auf die neueste Version zu aktualisieren, um weiterhin alle Funktionen und Sicherheitsstandards nutzen zu können.

Bitte klicken Sie auf den untenstehenden Button und folgen Sie den Anweisungen, um die Aktualisierung durchzuführen:

[Jetzt Aktualisierung APP](#)

Wichtig: Sie haben noch ein paar Tage Zeit, um das Update abzuschließen. Nach diesem Zeitraum können Einschränkungen bei der Nutzung der ING-Anwendung gelten. Um Unannehmlichkeiten zu vermeiden, bitten wir Sie, die Aktualisierung so schnell wie möglich durchzuführen.

Ihre Finanz-Nachrichten für den Dezember.

Sehr geehrter Kunde,

Wir möchten Sie nochmals daran erinnern, Ihre ING App auf die neueste Version zu aktualisieren, um weiterhin alle Funktionen und Sicherheitsstandards nutzen zu können.

Bitte klicken Sie auf den untenstehenden Button und folgen Sie den Anweisungen, um die Aktualisierung durchzuführen:

Jetzt Aktualisierung APP

Wichtig: Sie haben noch ein paar Tage Zeit, um das Update abzuschließen. Nach diesem Zeitraum können Einschränkungen bei der Nutzung der ING-Anwendung gelten. Um Unannehmlichkeiten zu vermeiden, bitten wir Sie, die Aktualisierung so schnell wie möglich durchzuführen.

Sehr geehrter Kunde,

Aus Sicherheitsgründen haben wir den Zugriff auf Ihr Konto gesperrt, da Sie Ihre Telefonnummer nicht bestätigt haben.

Ihre nächsten Schritte:

Bestätigen Telefonnummer

Bei Fragen steht Ihnen unser Kundenservice gerne zu Verfügung. Senden Sie eine E-Mail an kundenservice@c24.de oder rufen Sie uns unter folgender Telefonnummer an: 069 24 24 69 000 (Mo. bis Fr. 8:00 – 20:00 Uhr).

Wir freuen uns, Sie schon bald als aktiven Kunden begrüßen zu dürfen!

Viele Grüße
Ihre C24 Bank

Sehr geehrter Kunde,

Aus Sicherheitsgründen haben wir den Zugriff auf Ihr Konto gesperrt, da Sie Ihre Telefonnummer nicht bestätigt haben.

Ihre nächsten Schritte:

Bestätigen Telefonnummer

Bei Fragen steht Ihnen unser Kundenservice gerne zu Verfügung. Senden Sie eine E-Mail an kundenservice@c24.de oder rufen Sie uns unter folgender Telefonnummer an: 069 24 24 69 000 (Mo. bis Fr. 8:00 – 20:00 Uhr).

Wir freuen uns, Sie schon bald als aktiven Kunden begrüßen zu dürfen!

Viele Grüße
Ihre C24 Bank

Betrugsversuche („Scam“ und „Scareware“)

- **meist per E-Mail, SMS, Messenger (z.B. WhatsApp)**
- **„Enkeltrick“**
- **angebliche Gewinne, Spenden, günstige Kredite, ...**
- **angeblich sehr lukrative Geldanlagen**
- **angebliche Vireninfektionen („Scareware“)**

Digitale Sicherheit

„Enkeltrick“

Enkelkind oder Kind meldet sich angeblich mit einer neuen Handynummer.

Wenn man antwortet, erfährt man, dass das (Enkel)Kind angeblich dringend Geld braucht (z.B. Kaution nach einem Unfall).

Mittwoch, 27. Nov. • 04:20

SMS/MMS-Austausch mit [REDACTED]

Hallo,Mama und Papa dies ist meine neue
Rufnummer,bitte schreib mir eben eine
test-nachricht auf Whatsapp +49 [REDACTED]

04:20



SMS-Nachricht



Digitale Sicherheit

Gewinne, Spenden, Kredite, ...

Einfache Regeln:

- **Niemand hat etwas zu verschenken.**
- **Es gibt keine Lotterien, wo man – ohne vorher gefragt zu werden – teilnimmt.**
- **Wenn man antwortet, soll man erstmal eine „kleine“ Gebühr bezahlen, bevor der große Gewinn angeblich ausgezahlt werden kann.**

Lieber Freund info,

Ich bin Mr. Scott Godfrey, der Mega-Gewinner von 699 Millionen Dollar beim Mega Millions Jackpot. Wenn Sie diese E-Mail erhalten, wurde Ihre E-Mail nach einem Spinball ausgewählt. Ich habe den Großteil meines Vermögens an eine Reihe von Wohltätigkeitsorganisationen und Organisationen verteilt. Ich habe mich freiwillig dazu entschieden, Ihnen den Betrag von (zwei Millionen fünfhunderttausend Dollar) an einen der ausgewählten 5 zu spenden. Um meine Gewinne zu überprüfen, sehen Sie sich meine YouTube-Seite unten an.

SEHEN SIE MICH HIER AN: <https://www.youtube.com/watch?v=SET8O748k-U>

Dies ist Ihr Spendencode: [SC78924GB2024]

Antworten Sie auf diese E-Mail mit dem Spendencode: **office@scottgodfreyfoundation.com**

Ich hoffe, Sie und Ihre Familie glücklich zu machen.

Gruße

Mr. Scott Godfrey; Wednesday 1st January

Guten Tag, meine Damen und Herren.

Es ist wieder die Zeit des Jahres, in der Philip Marery zuverlässige Kreditangebote zu einem günstigen Zinssatz von 0,5 % für einen Zeitraum von 1 bis 40 Jahren herausgibt.

Es ist wieder die Zeit, in der jeder bei der Philip Marery Financial credit Company nach finanzieller Unterstützung suchen kann. Sowohl Kunden mit guter als auch mit schlechter Kreditwürdigkeit können sich bei dieser Kreditfirma bewerben.

Wir bieten Kredite wie Privatkredite, Firmenkredite, Geschäftskredite sowie Kredite für private und öffentliche Investoren an.

Wenn Sie also Interesse an einer Zusammenarbeit mit meiner Kreditfirma haben, erreichen Sie mich für weitere Informationen unter meiner unten angegebenen E-Mail-Adresse.

Kontaktieren Sie mich unter: financecompany@consultant.com

Mit freundlichen Grüßen
Management

Digitale Sicherheit

„Scareware“

Nachgemachte Meldungen einer angeblichen Vireninfektion.

Wenn man den Anweisungen zur Behebung der Infektion folgt, dann installiert man erst den richtigen Virus.

Digitale Sicherheit

Soziale Netzwerke

Keine persönlichen Informationen veröffentlichen (z.B. Geburtsdatum und -ort, Mädchennamen, Ehestand, Adresse, Telefonnummer).

Diese Informationen können von Identitätsbetrügern missbraucht werden.

Digitale Sicherheit

Soziale Netzwerke

Vorsicht vor Freundschaftsanfragen von Fremden:

- **Jeder kann sich dort irgendeinen Namen aussuchen.**
- **Man weiß nie, wer wirklich dahinter steckt.**
- **Unbekannten niemals mit Bankgeschäften helfen!**

Betrüger suchen gerne in sozialen Netzwerken nach Opfern!

Digitale Sicherheit

Soziale Netzwerke

Reißerische Schlagzeilen („click bait“) nicht glauben.

Absurde Meldungen nicht glauben („fake news“).

Angeblichen Beweis-Fotos nicht glaube, können KI-generiert sein.

Jeder kann dort „Nachrichten“ verbreiten, ganz ohne journalistische Ausbildung.

Soziale Netzwerke – digitale Hygiene

Wenn Sie ein soziales Netzwerk ausprobiert haben, aber nicht mehr verwenden wollen, löschen Sie Ihr Konto, anstatt es nur „brach“ liegen zu lassen.

Nur ein gelöschttes Konto ist absolut sicher davor, gekapert zu werden!

Fragen?

Ende!