



#Choose2BeSecureOnline

Sicher durchs Netz mit dem LRZ



E-Mails verschicken

Unverschlüsselte E-Mails sind
so sicher wie Postkarten...



Deshalb:

- ✓ Keine sensiblen Informationen versenden
- ✓ E-Mail-Verschlüsselung nutzen
- ✓ Dateien nicht als Anhang senden, sondern
(passwortgeschützte) Download-Links
nutzen (z. B. über LRZ Sync+Share)

Sending emails

Unencrypted emails
are as safe as postcards...



So:

- ✓ Do not send sensitive information
- ✓ Use email encryption
- ✓ Do not send files as attachments,
but use (password-protected)
download links (e.g. via LRZ Sync+Share)

E-Mail-Absender prüfen

Beim Erhalt von E-Mails immer:

- ✓ Domain/URL prüfen! Tippfehler im Absender sind verdächtig (z. B. @uni-muemchen.de statt @uni-muenchen.de).
- ✓ Stimmt der Anzeigename mit der Absenderadresse überein (z. B. Sparkasse Kundenservice <asldkf@aueng.de>)?

Pro-Tipp: Lerne Phishing-Mails zu erkennen (z. B. unter www.phish-test.de).



Check email sender

When receiving emails, always:

- ✓ Check domain/URL of the sender! Typing errors are suspicious (e.g. @uni-muemchen.de instead of @uni-muenchen.de).
- ✓ Does the shown name match the sender address (e.g. your Bank customer service <asldkf@aueng.de>)?

Pro tip: Learn to recognise phishing emails (e.g. at www.phish-test.de).



E-Mail-Anhänge & Links



- ✓ Anhänge aus unbekannter Quelle nicht öffnen
- ✓ Im Zweifel beim Absender nachfragen
- ✓ Wenn angehängte Dateien geöffnet werden, dann in der Leseansicht
- ✓ „Hier klicken“ könnte überall hinführen!
 - Links/Buttons/Bilder prüfen
 - Vorsicht bei Shortlinks wie z. B. bit.ly

Email Attachments & Links



- ✓ Do not open attachments from unknown sources
- ✓ Ask the sender if unsure
- ✓ If attached files are opened, then in read-only view
- ✓ „Click here“ could lead anywhere!
 - Check links/buttons/pictures
 - Be careful with shortlinks such as bit.ly

Passwort-Qualität

Bei der Passwort-Wahl beachten:

- ✓ Länge schlägt Komplexität!
- ✓ 12 Zeichen oder mehr
- ✓ Zeichenraum ausnutzen: Buchstaben groß und klein, Zahlen und Sonderzeichen
- ✓ Für jeden Dienst/Webseite ein eigenes Passwort

Wie merke ich mir ein Passwort?
Satz bilden und Anfangsbuchstaben
und Zahlen als Passwort nutzen.



Password quality

Keep in mind:

- ✓ Length beats complexity!
- ✓ 12 characters or more
- ✓ Use full character range: Upper and lower case letters, numbers and special characters
- ✓ A separate password for each service/webside

How do I remember a password?
Form a sentence and use the first
letters and numbers as a password.



Passwörter schützen



- ✓ Passwörter niemals...
 - an Dritte weitergeben
 - auf Zettel schreiben und an Monitor oder Tastatur kleben
- ✓ Passwortmanager wie KeePass nutzen
- ✓ Private und dienstliche Passwörter getrennt verwalten
- ✓ Wenn möglich, Zwei-Faktor-Authentifizierung einrichten

Protecting passwords



- ✓ Never...
 - give a password to anyone else
 - note a password down and stick it to your monitor or keyboard
- ✓ Use a password manager such as KeePass
- ✓ Manage private and work-related passwords separately
- ✓ If possible, set up two-factor authentication

Eigenes WLAN

- ✓ Verschlüsselungsstandard WPA2 oder WPA3 verwenden
- ✓ Komplexes und langes WLAN-Passwort (mind. 20 Zeichen) wählen
- ✓ Für Gäste einen Gastzugang einrichten



Your WIFI

- ✓ Use the encryption standard WPA2 or WPA3
- ✓ Generate a complex and long WIFI password (at least 20 characters)
- ✓ Set up guest access for guests



Öffentliches WLAN

In öffentlichen Netzwerken kann mitgelesen werden!

Deshalb:

- ✓ Online-Banking in öffentlichen WLANs vermeiden
- ✓ Privatssphäre schützen: VPN verwenden
- ✓ Vor der Passworteingabe die URL prüfen: Wird ein sicheres Kommunikationsprotokoll (HTTPS) verwendet?



Public WIFI

Public networks are open to read!

Therefore:

- ✓ Avoid online banking in public WIFIs
- ✓ Protect your privacy: Use VPN
- ✓ Check URL for secure communication protocol (HTTPS) before entering a password



Arbeiten im Homeoffice

- ✓ Immer via VPN ins Instituts- oder Firmennetz einwählen
- ✓ Für dienstliche Aufgaben dienstliche Geräte verwenden
- ✓ Wird der Arbeitsplatz verlassen: Bildschirmsperre mit Passwort-Eingabe aktivieren (Windows-Taste + L, Mac: CTRL + CMD + Q)



Working from Home

- ✓ Always use VPN when you log-in to your institute or company network
- ✓ For work-related tasks use company devices
- ✓ When leaving the workplace: Activate screen lock with password prompt (Windows key + L, Mac: CTRL + CMD + Q)



Sicher im Internet surfen



- ✓ Persönliche Daten und Passwörter nur eingeben, wenn HTTPS in der URL
- ✓ Webseiten kritisch prüfen:
 - Impressum vorhanden?
 - Auftritt seriös?
 - Domain plausibel?
- ✓ Keine „kostenlosen“ Virenskans durchführen
- ✓ Werbeblocker für Browser verwenden

Surf the internet safely



- ✓ Enter personal data and passwords only when HTTPS in the URL
- ✓ Check websites:
 - Imprint available?
 - Serious appearance?
 - Domain plausible?
- ✓ Do not run „free“ virus scans
- ✓ Use ad blocker for your browser

Anti-Viren-Software

- ✓ Installation von Anti-Viren-Software nur aus vertrauenswürdiger Quelle
- ✓ Auf regelmäßige, automatische Updates der Virensignaturen achten
- ✓ Regelmäßige Durchführung von Scans
- ✓ On-Access-Scan aktivieren



Anti-Virus Software

- ✓ Install anti-virus software only from trustworthy sources
- ✓ Ensure regular, automatic updates of virus signatures
- ✓ Carry out regular scans
- ✓ Activate on-access scanning



Erste Hilfe bei Virenbefall

- ✓ Ruhe bewahren!
Keine vorschnelle Reaktion
- ✓ PC/Laptop vom Internet trennen
- ✓ Kein Onlinebanking mit befallenem System –
Eingaben könnten mitgelesen werden!
- ✓ Beruflich: Zuständige Stellen informieren
Privat: Scan der Anti-Viren-Software starten



First Aid for Virus Attacks

- ✓ Keep calm! No hasty reaction
- ✓ Disconnect computer from Internet
- ✓ No online banking with infected
system – entries could be monitored!
- ✓ At work: Inform the responsible authorities
At home: Start anti-virus scan



Daten richtig sichern

- ✓ Regelmäßige Backups von den wichtigsten Dateien durchführen
- ✓ 3-2-1-Regel: 3 Kopien auf 2 verschiedenen Datenträgern (z. B. USB-Stick), davon 1 außer Haus (z. B. LRZ Sync+Share)
- ✓ Zugriff und Wiederherstellung von Backups testen (funktioniert alles?)



Back up data properly

- ✓ Back up the most important files on a regular basis
- ✓ 3-2-1 rule: 3 copies on 2 different media types (e.g. USB stick), of which 1 is off-site (e.g. LRZ Sync+Share)
- ✓ Test access and restore of backups (does everything work?)



Installation von Software

- ✓ Download nur aus vertrauenswürdigen Quellen
- ✓ Auf kostenlose „PC-Beschleuniger“ verzichten
- ✓ Im Alltag kein Administrator-Konto nutzen
- ✓ Nicht mehr benötigte Software deinstallieren



Installing Software

- ✓ Download only from trusted sources
- ✓ Avoid free „computer accelerators“
- ✓ Do not use an administrator account in everyday life
- ✓ Uninstall software that is no longer needed



Künstliche Intelligenz



- ✓ Keine vertraulichen Daten mit KI-Chatbots teilen, wenn Art der Verarbeitung unklar ist
- ✓ Einstellungen zur Privatsphäre prüfen und ggf. anpassen
- ✓ KI-Antworten kritisch bewerten und hinterfragen
- ✓ Im beruflichen Umfeld nur freigegebene KI-Tools verwenden

Artificial Intelligence



- ✓ Do not share confidential data with AI-chatbots if the nature of the data processing is unclear
- ✓ Review and, if necessary, adjust privacy settings
- ✓ Critically evaluate and question AI-generated responses
- ✓ Use only approved AI tools in a professional environment

Impressum

Herausgeber

Leibniz-Rechenzentrum
der Bayerischen Akademie der Wissenschaften
Boltzmannstraße 1
85748 Garching b. München

www.lrz.de



Leibniz-Rechenzentrum
der Bayerischen Akademie der Wissenschaften