SAFETY CARD HOMEOFFICE

G DATA | TRUST IN GERMAN SICHERHEIT

Grundsätzliche Verhaltensrichtlinien

Verbindliche IT-Sicherheitsregeln

Sichere (VPN-) Verbindung

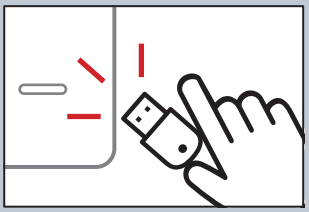
Sichere Kommunikationskanäle

Gefährdung durch Phishing vermeiden

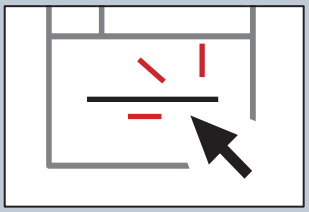
Gefährdung durch Viren vermeiden

Keine Chance für Cybercrime

Während der Verbindung mit dem Firmennetz



Keine **unbekannten Wechselmedien** verwenden



Keine **verdächtigen Links** anklicken

Unbeaufsichtigte Geräte immer **sperren**

Größte Vorsicht bei allen **E-Mail Anhängen**

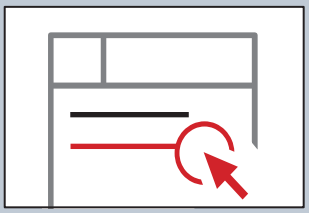
Einwahl nur über gesicherte Verbindung. Nur offizielle **Cloud-Tools** verwenden

Bei der Kommunikation in Chats etc. möglichst keine **persönlichen** Informationen

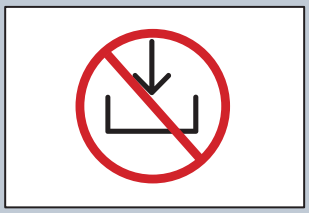
Lange Passwörter verwenden (für jeden Account ein eigenes), **Passwort-Manager** nutzen

Phishing-Versuche erkennen und abwehren

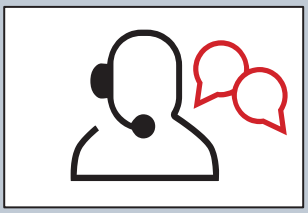
Bei Verdacht prüfen: **Ist die Absenderadresse gefälscht?**



Weichen die **sichtbaren Links** von den **echten Linkzielen** ab?



Keine **unerwarteten Dateien** oder Anhänge herunterladen



Im Zweifel **immer bei der IT-Abteilung melden**

Vorsicht bei allen E-Mails mit aktuellem Bezug, die **Angst machen** (z. B. COVID-19)

Bei Betreff und Inhalt von E-Mails auf **Fehler** und **Ungereimtheiten** achten

Richtiges Handeln im Notfall

Verwendetes Gerät **sofort vom Netzwerk trennen**, evtl. weitere Geräte prüfen

IT-Abteilung umgehend telefonisch kontaktieren und den Sachverhalt schildern

Betroffene Geräte bis zur Klärung der Situation nicht weiter nutzen, auch nicht offline

Anweisungen der **IT-Crew** beachten! | **Mehr Tipps** zum Homeoffice unter **www.gdata.de** |