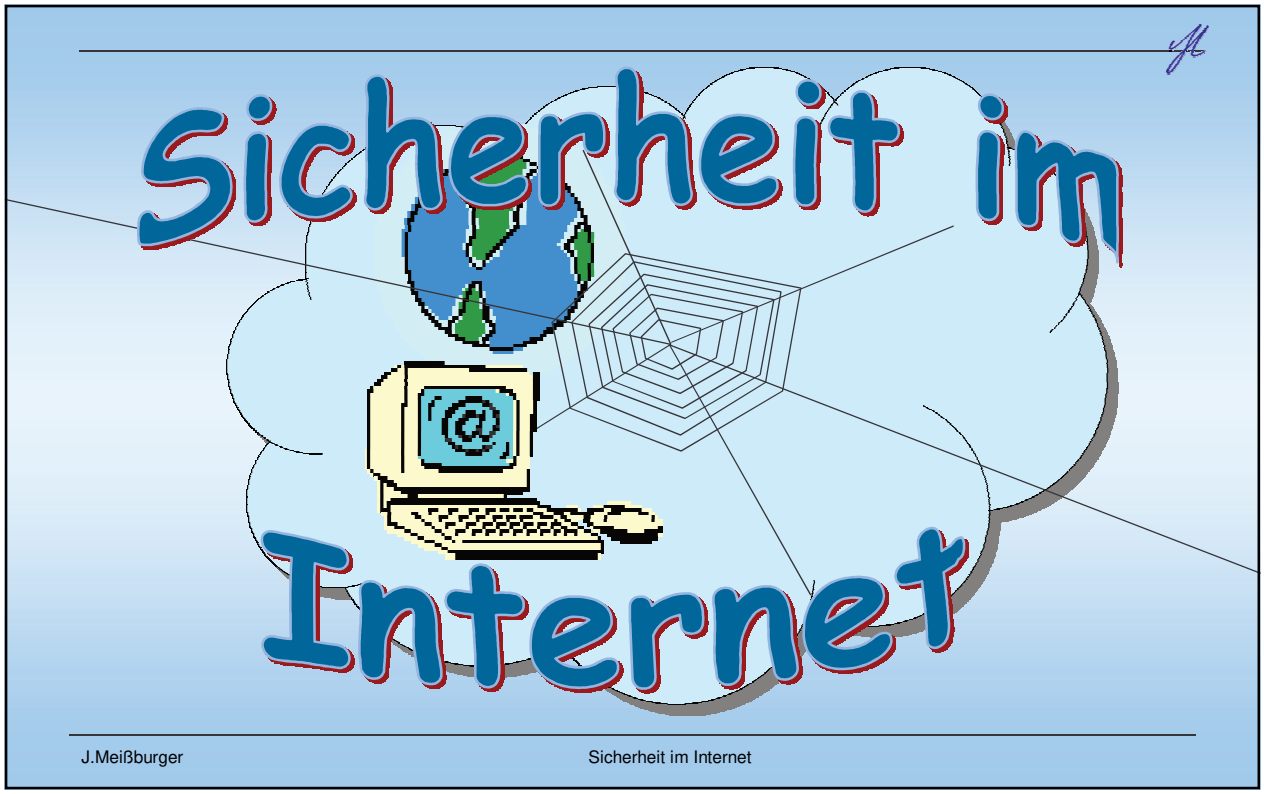


die größten Gefahren…

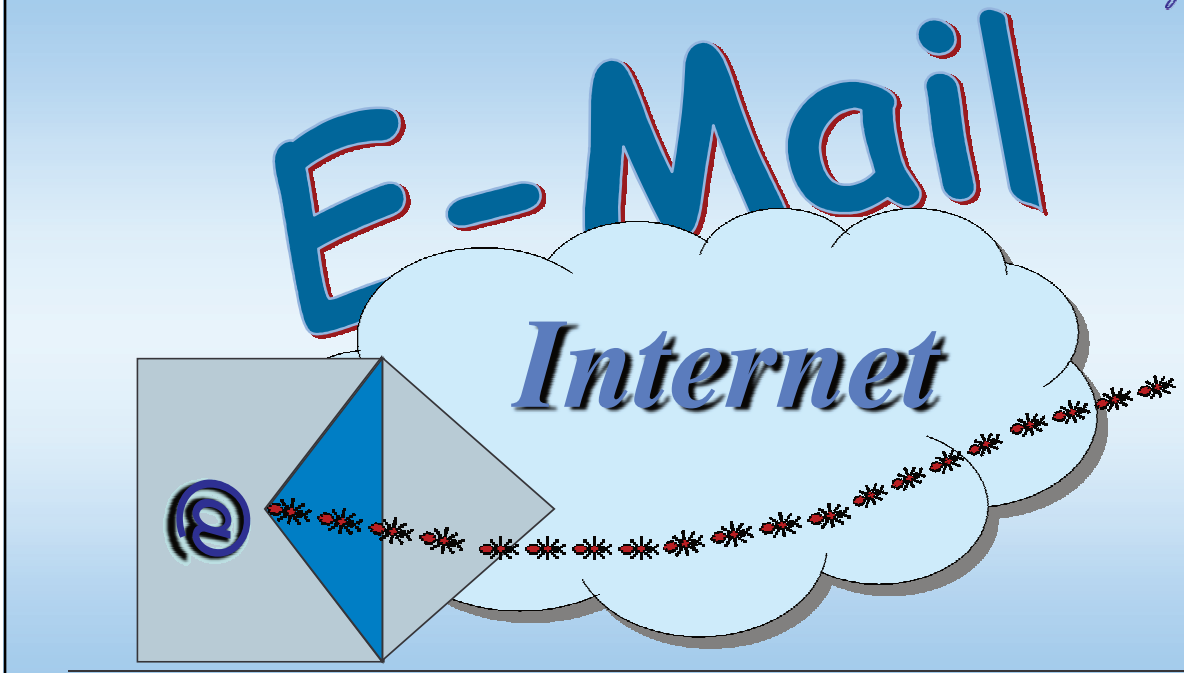
- Email: Installation von Schadsoftware bereits durch Vorschau oder Öffnen der Email oder eines Anhangs.
- Am gefährlichsten: Trojaner, die vollen Zugriff auf das System und alle Daten von außen erlauben (backdoor, exploit, rootkit).
- Abgreifen und Missbrauch vertraulicher Daten durch Phishing (Online-Shops, Bankkonten).
- Identitätsdiebstahl durch „password cracking“ oder gar durch Diebstahl biometrischer Daten (Fingerabdruck, Profilfoto!).
- Datenklau: Installation von Schadsoftware über präparierte Webseiten, PDF- oder Office-Dokumente.
- Preisgabe vertraulicher Daten in ungeschützten öffentlichen Netzen.
- Offenlegung nicht sicher gelöschter Daten.

J.Meißburger Sicherheit im Internet

und weiter …

- Daten- und Identitätsdiebstahl bei Geräteverlust, z.B. bei Diebstahl oder Reparatur!
- Datenverlust durch Hard- und Softwarefehler.
- Kompletter System- und Datenverlust durch Ransomware (Verschlüsselung der Festplatte).
- Missbrauch in einem Botnet (Spam, DDoS).
- Kostenfallen, ungewollte Abos (google playstore!).
- Rufschädigung, Mobbing in sozialen Netzen.
- Preisgabe persönlicher Daten durch fremden Zugriff auf das Heimnetz (Router, Smart-TV, UPnP)

J.Meißburger Sicherheit im Internet



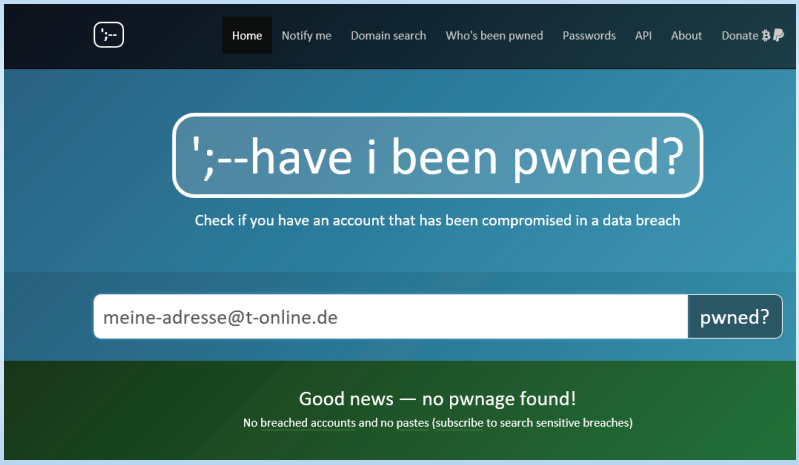
J.Meißburger Sicherheit im Internet

E-Mails immer misstrauen !!!

- Absender und E-Mail können gefälscht sein.
- Emails können Ihren Rechner mit Schadsoftware infizieren.
- Deshalb:
- Absender und Betreff sorgfältig auf Sinnhaftigkeit prüfen.
- Nicht auf Links in Email unbekannter Herkunft klicken.
- Auf Spam-Emails niemals antworten!
- Besondere Vorsicht vor Phishing E-Mails, die mit gefälschten Login-Seiten vertrauliche Daten anfordern !
- Zweifelhafte Emails sofort unbesehen löschen !
- ➔ Weder Ihre Bank, noch das Bundeskriminalamt oder die Polizei werden Ihnen jemals eine Email schicken !!!

Email-Adresse gehackt ?

- Troy Hunt (Have I been pwned?)



- Siehe ZDF-Mediathek, Film 510439 vom 17.1.2019

Smartphones, Smart-TV

- Sperrcode und Gerätemanager einrichten.
- Apps und Einstellungen auf PC oder in del Cloud sichern.
- Kein Rückruf auf unbekannte Nummern!
- Unnötige App-Rechte nach Installation entfernen (Ab Android 6.0)!
- Zugriff auf sensitive Daten vor Abgabe des Geräts verhindern (SIM/SD-Karte entfernen, Gerät rücksetzen)! Nicht ausleihen!
- Vorsicht in öffentlichen, ungeschützten WLAN-Netzen: Mitschneiden des Datenverkehrs durch Fremde!
- Vertrauliche Gespräche nur über verschlüsselte Verbindungen führen. Bei DECT-Telefonen stets DECT-Verschlüsselung aktiv!
- Funk (WiFi, Bluetooth, NFC) und GPS deaktivieren.
- ➔ Achtung: Die Telefonnummer eines Anrufers oder des Absenders einer SMS können gefälscht sein !!!

J.Meißburger Sicherheit im Internet

Vorsorge ist besser als …. !

- Für alle Konten unterschiedliche Passwörter >12 und 2FA
- Automatische Updates überprüfen.
- Systemwiederherstellung für „C:“ aktivieren.
- Systemabbild und (einmalig) Reparaturdatenträger erstellen .
- Internet-Zugang absichern („guter“, d.h. >21 WPA-Schlüssel).
- Smartphones vor Weitergabe verschlüsseln und rücksetzen !
- „gute“ Internet-Security-Suite installieren.
- Regelmäßig (evtl. automatisch) Benutzerdaten sichern.
- Sensitive Daten auf dem Rechner und in der Cloud „gut“ verschlüsselt ablegen.
- Sensitive Daten niemals unverschlüsselt über Email versenden.

J.Meißburger Sicherheit im Internet

Sicherheit durch Verschlüsselung

- Stets Transport-Verschlüsselung SSL/TLS verwenden!
- Sensitive Daten auf Datenträgern wie Festplatten, USB-Sticks oder in der Cloud grundsätzlich verschlüsseln!
- Größere Datenbestände (Ordner) oder ganze Festplatten mit VeraCrypt verschlüsseln:
  - Ordner samt Unterordner als Crypto-Container („volumes“).
  - USB-Sticks oder Festplattenpartitionen ggf. komplett.
- Passwörter bei Bedarf in einem Passwort-Manager wie „Keepass Password Safe“ abspeichern.Vorteile:
  - sichere, verschlüsselte Speicherung, nur ein Master-Passwort
  - Automatisches Login (Macro-programmierbar)
- Für Fotofreaks: Nachrichten verschlüsselt in Multimedia-Dateien verstecken (Steganografie)

Grundregeln beim Surfen im WWW

- Immer erst lesen, dann klicken …..
- Vor dem Klicken die Maus über das Link ziehen und die Statuszeile beobachten.
- Immer darauf achten, wo (IP-Domäne) man gerade surft: Adressleiste beobachten und nicht abschalten!
- Bei kritischen Transaktionen ausschließlich SSL-verschlüsselt arbeiten:
  - die Adresse muss mit https://…… beginnen!
  - neben der Adresse wird ein Schlosssymbol angezeigt
- Keine Passwörter oder Zahlungsmethoden im Browser speichern. Cookies und Verlauf nach Sitzungsende automatisch löschen.

Zwei-Faktor Authentisierung 2FA

- Konten-Zugang nur mit zwei unabhängigen „Tokens“.möglich,
- 1. Token: Übliche User-ID und (gutes) Passwort.
- 2. Token: Für ca. 20 Sek gültiger zusätzlicher Schlüssel:
  - durch Sprachnachricht an eine voreingestellte Telefonnummer
  - durch eine SMS oder Notiz an eine voreingestellte Telefonnummer
  - durch eine zusätzlich Passwort-geschützte App
  - durch einen elektronischen Key oder eine SmartCard
- Typische 2FA-Apps für Handy und PC:
  - Google Authenticator
  - Authy

YubiKey NEO mit NFC

- 2FA kann nachträglich für bestimmte Geräte wie z.B. den eigenen PC auch wieder deaktiviert werden.

J.Meißburger Sicherheit im Internet

Sicherheit bei PayPal: Profil - Einstellungen

- Email-Adressen überprüfen.
- Persönliche Daten: Handynummer eingegeben (für Sicherheitsschlüssel-Login,Verifizierung bei Problemen und 2FA).
- Bankdaten korrekt, keine unbekannten oder neue Einträge?
- Bankdaten: „PayPal-Zahlungen per Händlerabbuchung“ prüfen.
- „Einstellungen für Zahlungen über verbundene Mobilgeräte“ prüfen.
- „Benachrichtigungen“: Zahlungsbestätigungen“ alle aktivieren.
- „Login mit PayPal“: Mit dem PayPal Konto verknüpfte Seiten prüfen.
- Kundenservice-PIN für telefonische Anfragen einrichten.
- 2FA (leider nur über SMS möglich) aktivieren.

J.Meißburger Sicherheit im Internet

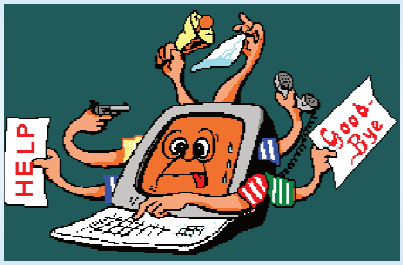
und überhaupt …

- Gelegentlich auf allen Geräten die Konten überprüfen.
- Geräte-Manager einrichten und aktivieren.
- Verbundene Geräte, wenn nicht gerade in Benutzung, möglichst abmelden (Google, Kindle, Music, Amazon).
- Profile aller wichtigen Konten überprüfen und anpassen.
- Unbenutzte Schnittstellen deaktivieren:
  - GPS, Standortdienste
  - WLAN
  - NFC
  - Bluetooth

Dateien und Ordner sicher löschen …

- Programm sdelete.exe von Microsoft downloaden:
  - https://docs.microsoft.com/de-de/sysinternals/downloads/sdelete
- Auf sdelete.exe "Rechte Maus - Verknüpfung erstellen„
- Auf der Verknüpfung "Rechte Maus - Eigenschaften"
  - Unter "Allgemein" den Namen der Verknüpfung ändern in "Sicher Löschen MS"
  - Unter "Verknüpfung" das Ziel ändern in "C:\Users\....\sdelete.exe -p 3 -s -q"
  - Unter "Erweitert" rechts unten Haken bei "Als Administrator ausführen" setzen
- 5. Die fertige Verknüpfung nach
  - "C:\Users\....\AppData\Roaming\Microsoft\Windows\SendTo" verschieben
- Damit erscheint die Funktion "Sicher löschen MS" im Kontextmenu z.B. eines Ordners oder einer Datei und kann direkt so benutzt werden.

System sichern



Systemwiederherstellung

- Erstellen von "Wiederherstellungspunkten" zum Rückgängigmachen fehlerhafter System- und Softwareänderungen.
- Eigene gelöschte Dokumente werden dabei nicht wiederhergestellt!
- Wiederherstellungspunkte werden gelegentlich auch automatisch durch Windows (z.B. vor kirtischen Updates) erstellt.
- Wiederherstellungspunkte sollten aber unbedingt ***vor jeder Installation neuer Software*** von Hand erstellt werden!
- Die Wiederherstellung sollte auf allen Festplatten außer der Systemplatte „C:“ deaktiviert sein.
- Die Systemwiederherstellung ersetzt kein Systemabbild !!!
- Vor einer Wiederherstellung Selbstschutz und Autostart der Antiviren-Software deaktivieren!

Betriebssystem sichern (Systemabbild)!

1. Wiederherstellungspunkt erstellen:
   - Cortana – Wiederherstellungspunkt erstellen.
2. Festplatte bereinigen (schafft Platz!):
   - Cortana – Datenträgerbereinigung.
3. Festplatte(n) auf Fehler überprüfen und ggf. reparieren:
   - „Dieser PC“ öffnen – Festplatte C: - RM – Eigenschaften – Tools – Prüfen.
   - Rechner neu starten und Prüfprogramm laufen lassen.
4. Betriebssystem sichern:
   - Externe USB-Festplatte NTFS-formatiert anschliessen.
   - Cortana – Sichern und Wiederherstellen – Systemabbild erstellen – USB-Festplatte auswählen – Weiter

- Zum Schluss einmalig leere DVD einlegen und „Systemreparaturdatenträger erstellen“ und sicher verwahren.

nochmal Android …

- SIM Kartensperre aktivieren.
- Displaysperre aktivieren (nicht biometrisch!).
- Unbekannte Apps installieren – nicht zulässig.
- Zugriff auf Nutzungsdaten – nur Apps, die‘s brauchen.
- Uneingeschränkter Datenzugriff – Carrier Services.
- Geräteadministator-Apps einrichten und überprüfen.
- „Gerät finden“ testen.
- App „Sichern und Wiederherstellen“  installieren und Sicherung lokal, danach Kopie auf PC erstellen.