Sicherheit bei Internet-Nutzung

- Natürliche Vorsicht walten lassen
- Programme: Firewall, Virenscanner
- Viren, Ransomware
- Passwörter: richtige Wahl
- Programme aktuell halten: Update

Zur Wiederholung ein

Hinweis

Haben Sie keine Sorge, dass Sie
kaputt machen könnten

Haben Sie keine Sorge, dass Sie
ein Programm falsch bedienen könnten

Ein Tablet ist

bei normaler Behandlung

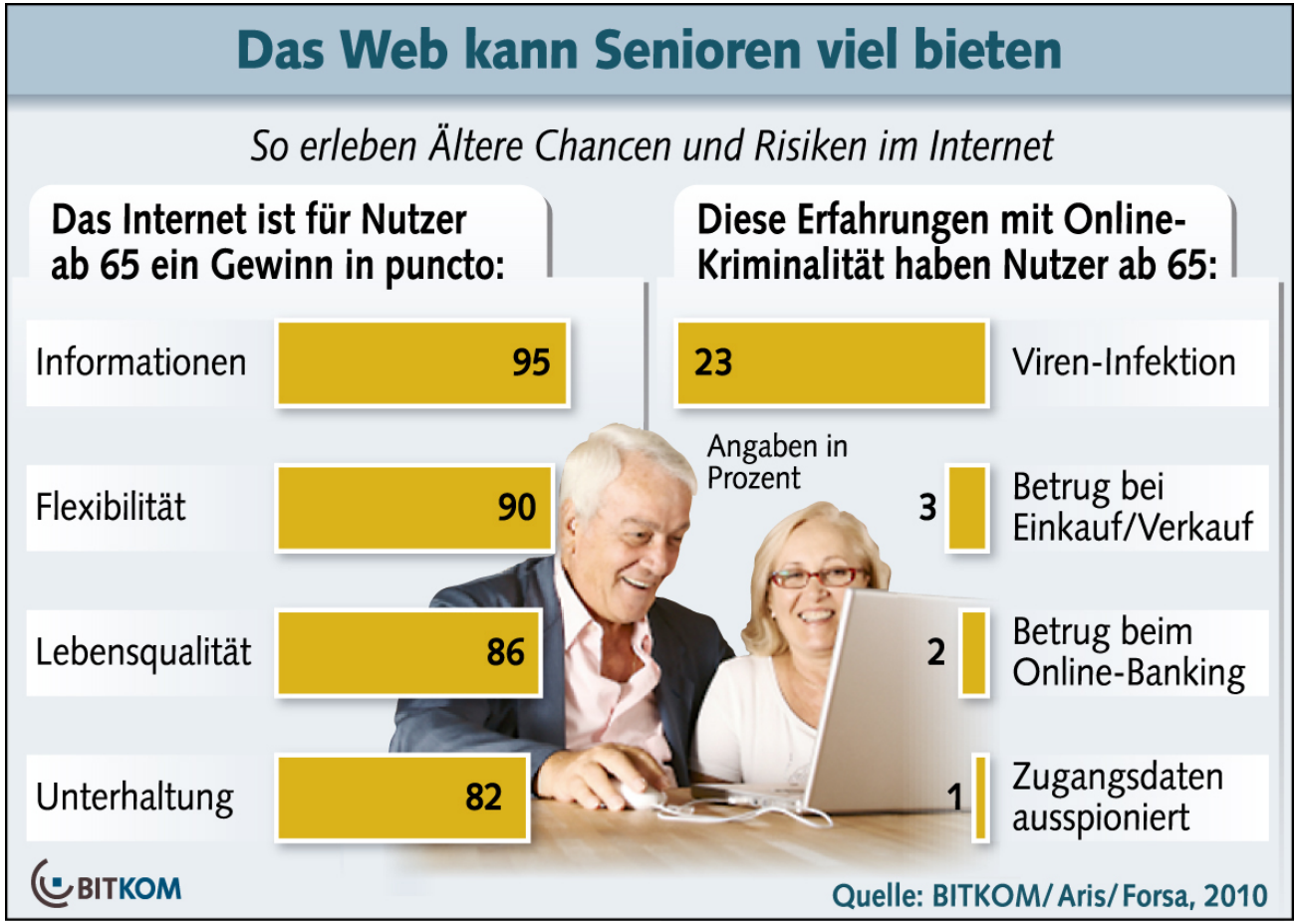
(fast) unkaputtbar

Die Programme sind

(nahezu) absturzsicher

Die Gefahrenstellen erfahren Sie gegebener Zeit

Nutzen und Risiken



Sicherheitsrisiken

- Beim „E-Mailen“ schicken uns auch Fremde eine E-Mail, manchmal auch **Verbrecher**
- Beim Installieren neuer Programme aus dem Internet können Schadprogramme dabei sein
- Beim Übernehmen von Bildern oder Musik von Freunden können Viren importiert werden

Also Vorsicht!

Sie müssen aber nun nicht zittern:

Mit etwas

Vorsicht

und

gesundem Menschenverstand

ist man auch in Internet sicher

Daher also zuerst

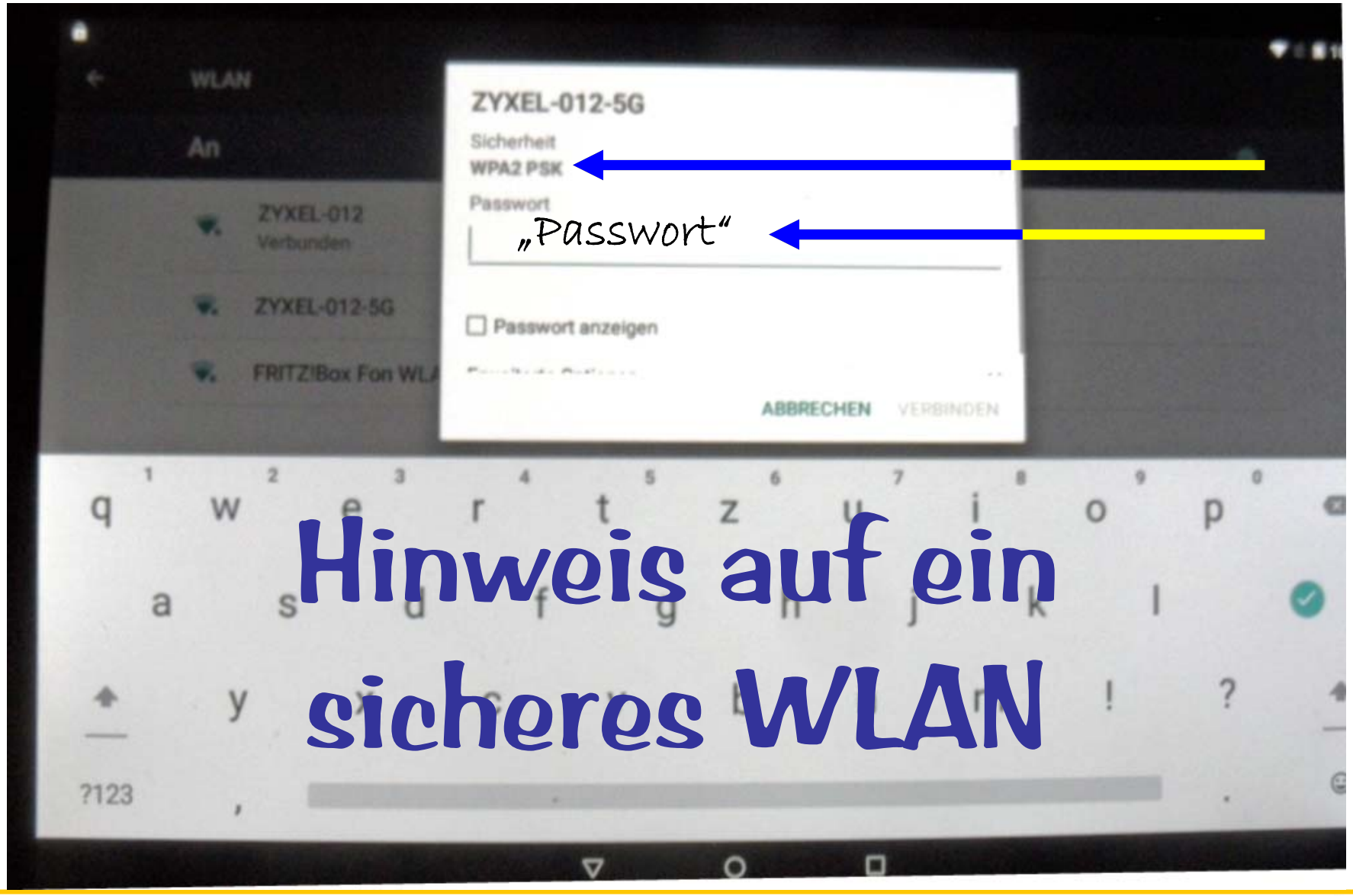
Sicherheit im Internet

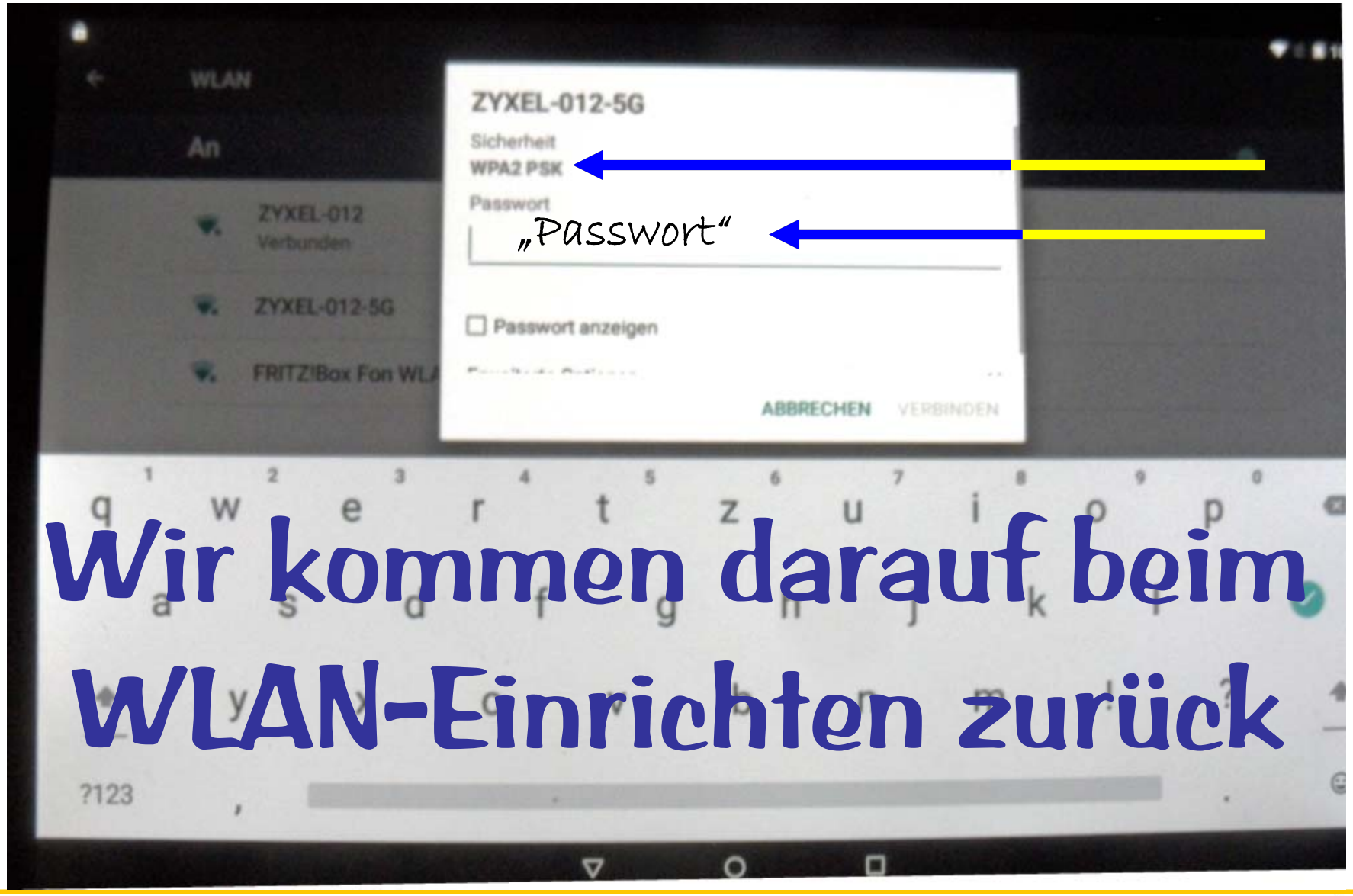
1. Punkt: Sicheres WLAN

Verbinden Sie sich nur über ein sicheres WLAN!

Lassen Sie sich zu Hause ein ein sicheres WLAN einrichten!

Verbinden Sie sich unterwegs nur über ein sicheres WLAN!


WLAN
An
ZYXEL-012
Verbunden
ZYXEL-012-5G
FRITZ!Box Fon WLA
ZYXEL-012-5G
Sicherheit
WPA2 PSK
Passwort
„Passwort“
Passwort anzeigen
ABBRECHEN
VERBINDEN
Hinweis auf ein sicheres WLAN


WLAN
An
ZYXEL-012
Verbunden
ZYXEL-012-5G
FRITZ!Box Fon WLA
ZYXEL-012-5G
Sicherheit
WPA2 PSK
Passwort
„Passwort“
Passwort anzeigen
ABBRECHEN
VERBINDEN
Wir kommen darauf beim WLAN-Einrichten zurück

2. Punkt: Passwort

Wenn Sie ein WLAN einrichten müssen Sie ein Passwort wählen.

Das ist Ihr eigenes Passwort!

Wählen Sie ein sicheres Passwort und geben Sie es nicht weiter!!!

Sicheres Passwort

Ein einfaches Passwort zu knacken ist keine schwierige Aufgabe für Kriminelle, also nicht:

~~1234567890~~

oder

~~Geburtsdatum~~

der

~~Namen~~

Sicheres Passwort

Ein sicheres Passwort ist

- mindestens 8 Zeichen lang, besser 10 oder 12
- enthält große und kleine Buchstaben
- enthält Sonderzeichen wir %, §, * usw.
- ist aus keiner Vorlage abgeschrieben

3. Punkt: Viren
Sicherheits-Software

Kriminelle versuchen oft Schadprogramme auf Ihr Tablet zu bringen. Beispiele hierfür sind:

- Computerviren: Schreiben sich in Programme
- Ransome-ware sind Erpresserprogramme
- Key-logger spionieren die Eingabe aus
- Rechenzeit-Diebstahl

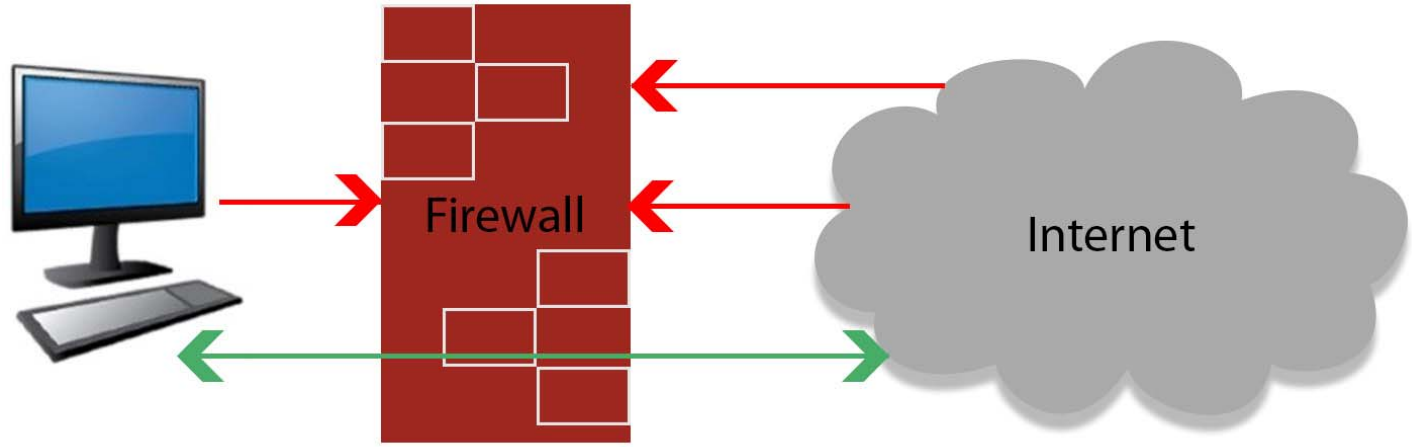
Sicherheit-Software

Zwei Programme sind wichtig:

- **Firewall**
  Die Firewall ist üblicherweise vorinstalliert.
  Sie hält Eindringlinge ab

- **Viren-Scanner**
  Ein Virenscanner sucht nach Viren-typischen Programmen oder Programmteilen

Firewall



unerlaubte Zugriffe werden von der Firewall blockiert
erlaubte Zugriffe werden zum Computer durchgelassen

Die Firewall verhindert unerlaubten Zugang zu den Geräten im internen Bereich, d.h. hinter dem Rooter in drei Zugangsstufen:

Offen (-) **Im WLAN-Bereich Offen (+/-)** **Nur Einzelzugang (+)**

Virenscanner

Der Begriff Viren wird heute für alle Arten von Schadprogrammen genutzt:

Viren sind Schadprogramme, die sich in Nutzprogramme einnisten und sich bei Aufruf des Programms vermehren und verbreiten. Zusätzlich richten sie den programmierten Schaden an, z.B. löschen sie Daten

Würmer sind Schadprogramme, die selbständig laufen, sich unabhängig vermehren und z.B. E-Mails mit einem Wurm verschicken.

Bots öffnen das Tablet (und die Firewall) für Fremde. Diese können dann auf dem Tablet rechnen oder auch E-Mails verschicken

Viren

Trojaner sind Schadprogramme, die anderen Rechnern einen Zugang zum Tablet öffnen und z.B. Passwörter ausspähen.

Ransom-ware sind Schadprogramme, die Daten auf dem Tablet durch Verschlüsseln unlesbar machen und den Besitzer erpressen. Aber: Nicht zahlen! Das Geld ist weg und entschlüsselt wird i.a. nicht.

Spy-ware späht die Daten (PIN, Passwörter) auf dem Tablet aus und schickt sie an die Verbrecher: Gefahr für das Bankkonto.

Warn-Mails sind E-Mails, die angeblich von Microsoft, Telekom, der Bank oder anderen Institutionen kommen und Warnungen vortäuschen, z.B. dass das Konto bald gesperrt wird. Es wird Hilfe über eine angegebene Verbindung angeboten. Sofort löschen!

Virenscanner

Hilfe gegen diese Gefahr*
bieten sogenannte Virenscanner

Virenscanner sind Programme, die im Hintergrund laufen und die die laufenden Apps und die Daten auf dem Tablet nach typischen Kennzeichen bekannter Viren absuchen.
Die Hersteller untersuchen jeden neuen Virus sofort und schicken - i.a. im Hintergrund – die Kennung zum Tablet.

Hersteller von Virenscannern sind z.B. Kaspersky, Avast, Norton, Bitdefender, AVG, GDATA u.a.

*** Virenscanner schützen nicht gegen Warn-Mails!**

4. Punkt: Datensicherung

Daten können verloren gehen,

- durch versehentliches Löschen

- durch Beschädigung des Tablets

- viele weitere Gründe

Datensicherung

Daten können Sie sichern

- auf einer zusätzlichen Speicherkarte

erinnern Sie sich an den Schlitz am oberen Rand

- durch Senden an einen 2. Rechner

erst wenn Sie lange Ihr Tablet benutzt haben

5. Punkt: Programm-Aktualisierung

- *Die Programme auf Ihrem Tablet werden von Menschen gemacht, d.h. sie können Fehler enthalten.*

- *Die Programme auf Ihrem Tablet können Sicherheitslücken haben durch die Kriminelle eindringen können.*

Programm-Aktualisierung

- Die Programm-Hersteller verbessern daher ihre Programme von Zeit zu Zeit.
- Sie erhalten dann ein sogenanntes „Software-Update“. Ihr Tablet zeigt Ihnen das an.
- Sie brauchen dann nur zustimmen, den Rest macht Ihr Tablet.

6. Herunterladen aus dem Internet

Seien Sie beim Herunterladen aus dem Internet vorsichtig:

Nur vertrauenswürdige Quellen nutzen

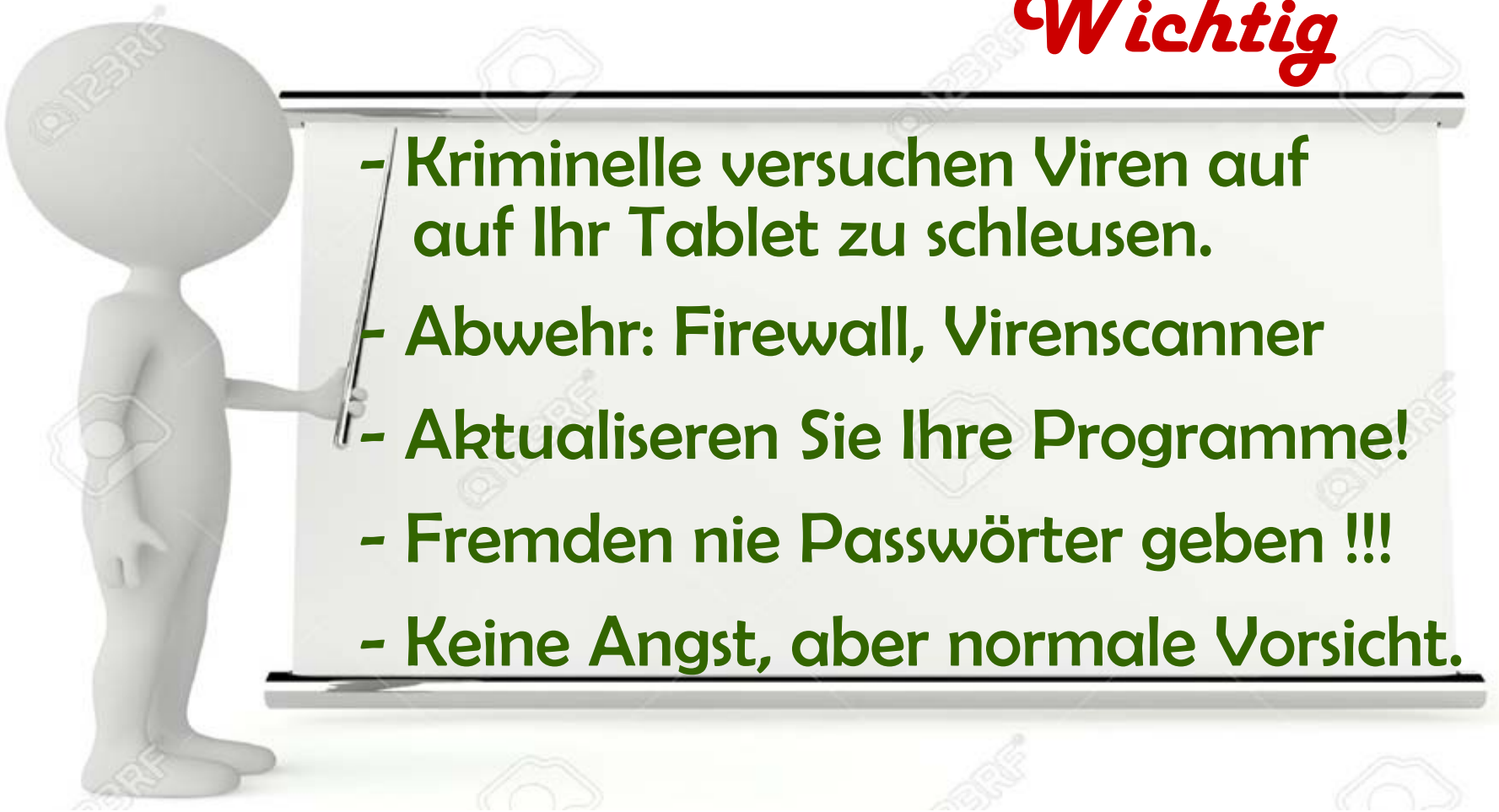
Ich habe beim letzten Mal genutzt:

Google, Youtube, Wikipedia, Vimeo

7. Anschließen einer fremden Quelle

Seien Sie vorsichtig, wenn Sie einen fremde Speicher, z.B. USB-Stick, anschließen:

Nur vertrauenswürdige Quellen nutzen und mit dem Virenscanner prüfen.


Wichtig
- Kriminelle versuchen Viren auf auf Ihr Tablet zu schleusen.
- Abwehr: Firewall, Virenscanner
- Aktualiseren Sie Ihre Programme!
- Fremden nie Passwörter geben !!!
- Keine Angst, aber normale Vorsicht.

Wir verbinden Sie

Die Bilder stammen z.T. vom BMFSFJ