

Nicht alle IT-Leute benutzen Ihre Kräfte für das Gute





## **Passwort Hacking**



RANG	PASSWORT	BENÖTIGTE ZEIT ZUM PASSWORT-KNACKEN
1	123456	< 1 Sekunde
2	password	< 1 Sekunde
3	123456789	< 1 Sekunde
4	12345	< 1 Sekunde
5	hallo	< 1 Sekunde
6	passwort	< 1 Sekunde
7	fi	< 1 Sekunde
8	12345678	< 1 Sekunde



# Phishing



### Platzierung und Fotos Halbmarathon Entenhausen!



Edwin Radtke <edwin@techstarter.de>
an mich ▼

#### Hallo liebe Arenda Könnecke,

Vielen Dank für eure Teilnahme am Entenhausen Halbmarathon. Anbei haben wir dir deine Bilder angehängt, die dich beim Zieleinlauf zeigen.

#### Du hast unter den Damen den 4 Platz belegt!

#### Damen - Top 10

Ochs, Katrin	02:58:07	W40
Fierek, Carina	03:01:28	W35
Eißmann, Mareike	03:20:39	W35
Könnecke, Arenda	03:23:04	W40
Schönherr-Holscher, Birgit	03:23:58	W50
Herzog, Simone	03:28:34	W40
Seidel, Renate	03:37:41	W55
Busch, Caren	03:42:17	W40
Rengers, Katja	03:44:18	W40
Hartrampf, Nicole	03:51:27	W35

#### Hier ist schon mal dein erstes Bild:



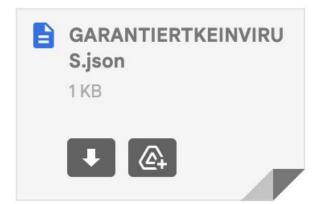
Wir freuen uns auf deine Teilnahme nächstes Jahr!

Dein Team Halbmarathon Entenhausen



#### Dein Team Halbmarathon Entenhausen

### Ein Anhang. Von Gmail gescannt (i)



## Öffentliches WLAN



## So funktioniert WLAN-Phishing

Nach dem Verbindungsaufbau mit einem WLAN rufen Smartphones und Notebooks automatisch eine HTTP-URL auf, um zu überprüfen, ob in dem Netz eine Portalseite (Captive Portal) geschaltet ist. Wenn ja, wird die Portalseite automatisch geöffnet. Ein Angreifer kann dem WLAN-Nutzer auf diese Weise leicht eine Phishing-Seite unterschieben.



Automatischer Verbindungsaufbau mit dem WLAN des Angreifers

Automatische HTTP-Anfrage: http://captive.apple.com/generate\_204

302-Umleitung zur bösartigen Site: https://apple-id-login-now.com

### Apple-ID

Bitte melde dich an, um mit der Nutzung fortzufahren.

otto@ct.de



Übertragung der Zugangsdaten an Angreifer Login: otto@ct.de, Passwort: G3h31m!





# Media Dropping

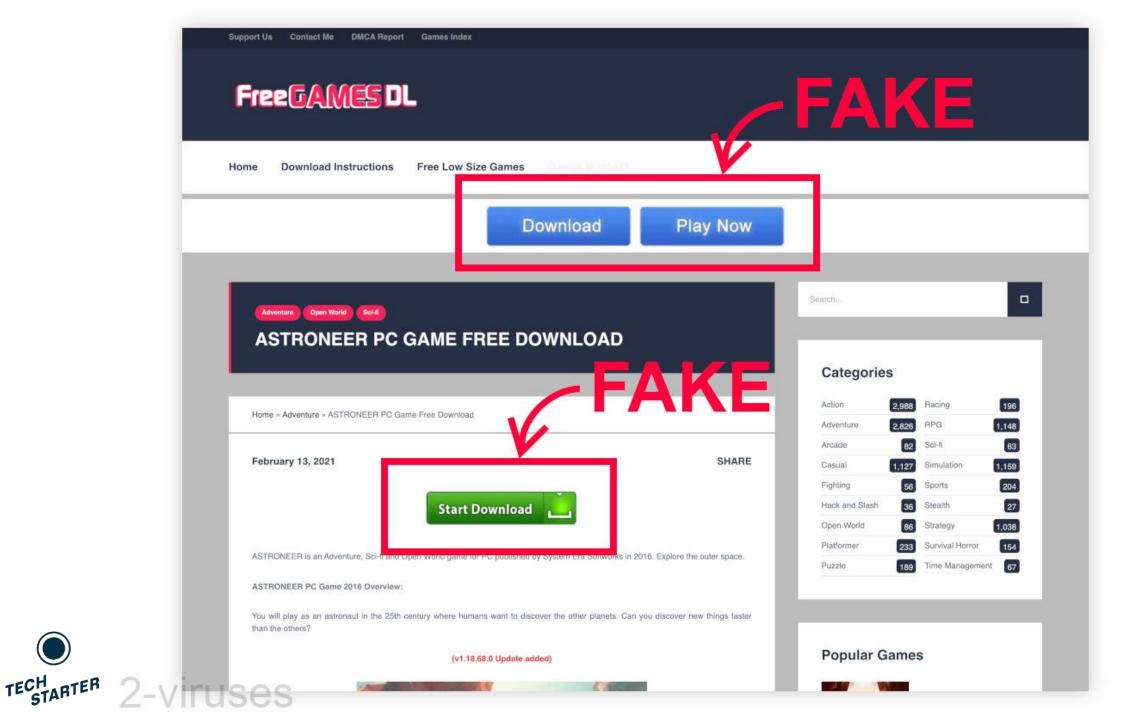






## Malware





# Vishing







## Basiselemente der IT-Sicherheit

### **Updates:**

Halten Sie Ihre Software durch Sicherheits-Updates auf dem neuesten Stand.

### Passwörter:

Verwenden Sie möglichst starke und unterschiedliche Passwörter. Hierfür können Sie einen Passwortmanager nutzen.

### Zwei-Faktor-Authentisierung:

Schützen Sie sich zweifach: Neben dem ersten Faktor, meist einem Passwort, nutzen Sie in einem zweiten Schritt z.B. Ihren Fingerabdruck oder eine TAN.

### Häufig vorhandener Schutz auf PCs und Laptops

### Virenschutzprogramm:

Es überprüft den gesamten Rechner auf Anzeichen einer Infektion.

#### Firewall:

Sie schützt vor Angriffen von außen und verhindert, dass Programme, z.B. Spyware, Kontakt vom Gerät zum Internet aufnehmen.

© Bundesamt für Sicherheit in der Informationstechnik (BSI)

www.bsi.bund.de

