SICHERHEITSKAMPAGNE
BMVg

SEI KEINE BEUTE!

LOGIN

Du bist die erste Verteidigungslinie, wenn es um Sicherheit geht. Achte darauf, dass Du Deine Daten in der Onlinewelt nicht fischen lässt und schütze damit unsere Bundeswehr!

bpaq.de/fisch

BUNDESWEHR

PHISHING

Online shoppen und zahlen findest Du super. Es ist auch so bequem. Aber Achtung: Es gibt viele Versuche, über gefälschte Webseiten, Emails oder Kurznachrichten sich Dein Vertrauen zu erschleichen und Deine Daten abzugreifen. Das kann richtig Geld kosten, von dem damit verbundenen Ärger einmal abgesehen.
Deshalb: Sei aufmerksam und falle nicht auf arnazon.de, bundesvvehr.de oder paypa1.com herein.

Schütze Dich und Deine Daten durch Deine Achtsamkeit!

bpaq.de/fisch

bpaq.de/bwm-ios
bpaq.de/bwm-apk

SICHERHEITSKAMPAGNE
BMVg

IMPRESSUM

Stab Informationsarbeit - Referat Öffentlichkeitsarbeit
Bundesministerium der Verteidigung

Stauffenbergstraße 18
10785 Berlin

Telefon: +49 (0) 30 2004-22236
Fax: +49 (0) 30 2004-22197

Bundeswehrkennzahl: 3400

www.bundeswehr.de

SICHERHEITSKAMPAGNE
BMVg

SEI KEINE BEUTE!

Du bist die erste Verteidigungslinie, wenn es um Sicherheit geht. Achte darauf, dass Du Deine Daten in der Onlinewelt nicht fischen lässt und schütze damit unsere Bundeswehr!

BUNDESWEHR

Umgang mit QR-Codes

QR-Codes findest du überall auf Postern, Werbung, Rechnungen. Das ist eine coole Erfindung und sehr bequem. Aber auch hier gilt: Prüfe, wer Dich auf seine Website locken will. Es gibt viele Versuche, sich Dein Vertrauen zu erschleichen und anschließend Deine Daten abzugreifen.
Deshalb: Sei misstrauisch, wenn Du QR-Codes siehst und nicht genau weißt, wer der Absender ist.

Schütze Dich durch ein gesundes Misstrauen!

Umgang mit Login-Daten

Du nutzt Deine dienstliche Mailadresse auch für Social Media? Das ist im dienstlichem Interesse vollkommen okay. Problematisch wird es, wenn Du dieselben oder auch nur ähnliche Passwörter benutzt wie für den Zugang zu Bw-Systemen. Das macht es für kriminelle Elemente und fremde Nachrichtendienste einfacher, unsere besonders geschützten Systeme anzugreifen.
Deshalb: Nutze komplexe und vor allem unterschiedliche Passwörter.

Schütze Dich und die Bundeswehr durch starke Passwörter!

Nutzung nicht zugelassener USB-Geräte

Du findest, dass an jeden Steckplatz auch etwas gesteckt gehört? Deine Tastatur und Maus müssen individuell sein? USB-Sticks dienen der schnellen Datenübertragung. Dem Besitzer kann man ja vertrauen? Tastaturen und Computermäuse lassen sich manipulieren. Bei USB-Sticks weißt Du nie, ob sich nicht doch schadhafte Software darauf befindet.
Deshalb: Nutze dienstliche Hardware und abgesicherte Schleusen-PCs. Das ist Dein Beitrag, die sichere Welt der Bw-IT noch sicherer zu machen!

Schütze Dich und die Bundeswehr durch Beachtung der Regeln!

Sichere mobile Kommunikation

Smartphones und mobiles Arbeiten sind Bestandteil unserer Arbeitswelt und nicht mehr wegzudenken. Das, was gesprochen wird, aber auch das, was auf dem Laptop zu sehen ist, kannst nicht nur Du hören und sehen. Es gibt viele zufällige oder interessierte Mithörende und -sehende in öffentlicher Umgebung. Aber auch Dein Dienstzimmer wird nicht nur von Dir aufgesucht, sondern auch von Serviceperpersonal und Besuchern.
Deshalb: Verhindere, dass Deine dienstlichen Gespräche mitgehört werden können und gib niemanden einen Einblick darauf, was gerade auf Deinem Laptop passiert.

Schütze Dich und Deine Organisation durch Deine Aufmerksamkeit!

Verhalten bei Anomalien

Du sitzt jeden Tag vor Deinem Dienstrechner. In letzter Zeit kommen dir Dinge merkwürdig vor. Deine Programme und Dateien sehen irgendwie anders aus. Du weißt aber nicht genau, warum. Zeit, Dir Hilfe zu holen! Wende Dich an den CSOCBw@bundeswehr.org. Dieses ist 24/7 besetzt und auch telefonisch unter Bw-Netz: 90 11111 Zivil: 02226 88-1245 oder 0800-05-11111 zu erreichen. Oder an Deinen Informationssicherheitsbeauftragten vor Ort. Dort wird Dir geholfen und schlimmere Folgen werden vermieden.

Schütze Dich und die Bundeswehr durch Achtsamkeit!