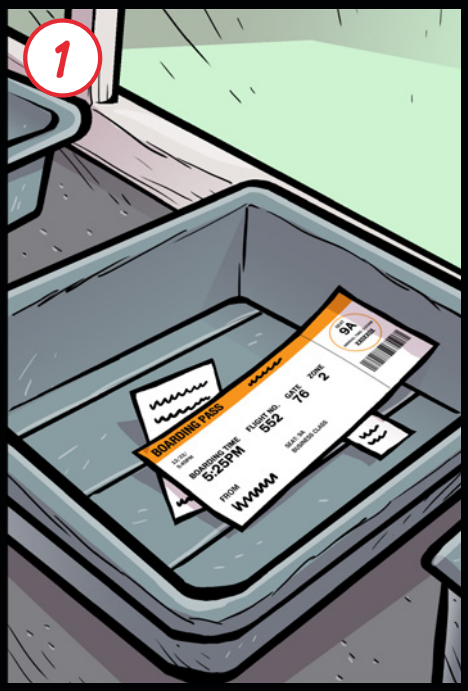
OpSec? Was ist das?!

MAL WIEDER EIN BUSINESS TRIP



KURZ VOR DEM ABFLUG...

4
Wie sehen ihre Umsätze aus?
Sehr gut so weit. Siehst Du?
Wow! Sieht sehr nach einer guten Ergänzung für uns aus.
5
Los geht's! Ich verhungere!
CLICK!
6
VORBEREITUNG FÜRS MEETING
Lass uns anfangen. Wir müssen morgen schon früh bei der Acme Corporation sein
7
Ich zahle mit Karte.
Wie war noch der verdammte PIN Code..?
Work: Address123!
Gmail: 123LastName
iPad: 9876
Pin: 5432
Bank: GB12 ABCD 3456 7890 1112 13
Card 1: 6789
Card 2: 5678
8

DER NÄCHSTE MORGEN

Acme Corporat

Guten Morgen! Wollen wir anfangen?

Ja, sehr gern.

SECURITY UPDATE

SKIP

9

NACH DER PRÄSENTATION

Können Sie mir bitte die Präsentation kopieren?

Klar!

rporation

10

Danke für Ihr Kommen.

Danke, wir melden uns bald.

rporation

DREI WOCHEN SPÄTER...

BUSINESS NEW

Acme Corporation acquired!

10 TIPPS FÜR BUSINESS OPSEC

1. Passen Sie immer gut auf Ihre Sachen auf. Alles, was ein Fremder braucht, um Ihren Reiseplan herauszufinden, ist ein Blick auf Ihren Nachnamen und die Buchungsreferenz auf dem Boarding Pass.

2. Verbinden Sie Ihre Geräte nur mit sicheren Ports. Wenn ein Port kompromittiert ist, gibt es keine Einschränkung für die Menge der Daten, die gestohlen werden oder Programme installiert werden können.

3. Nutzen Sie immer ein VPN um Ihren Datenverkehr zu schützen. Nutzen Sie Instant Messenger wie Signal Private Messaging, wenn Sie sensible Daten verschicken müssen.

4. Wählen Sie Orte, an denen Sie sich über geheime Dinge austauschen, mit Bedacht. Eine Person mit Noise-Cancelling Kopfhörern kann Ihre Diskussion auch trotz Lärm verfolgen.

5. Behalten Sie Ihre Geräte immer bei sich soweit möglich. Vermeiden Sie Safes in Hotels.

6. Nehmen Sie immer alle wertvollen Gegenstände und Arbeitsdokumente mit anstatt sie rumliegen zu lassen.

7. Überlegen Sie sich aktiv, was Sie teilen wollen, mit wem und wo. Selbst irrelevante Informationen können für andere interessant sein.

8. Speichern Sie Ihre Passwörter in einem Passwortmanager. Nutzen Sie generierte Passwörter, merken Sie sich die wichtigsten. Nutzen Sie niemals Passwörter nochmals.

9. Stellen Sie sicher, dass Ihr Betriebssystem immer auf dem neuesten Stand ist und stellen Sie automatische Updates an. Nutzen Sie möglichst iOS Geräte und Chromebooks und Chrome als Browser.

10. Verbinden Sie niemals unbekannte Peripheriegeräte mit ihren Geräten. Nicht einmal, wenn Sie den Eigentümer kennen.

Wirkungsvolle OpSec für einen längeren Zeitraum aufrecht zu erhalten, kann stressig sein. Viele Dinge müssen Sie immer wieder tun. Zusätzlich müssen Sie aufpassen, andere Dinge eben nicht zu wiederholen. Das ist nicht leicht. Aber vergessen Sie niemals: Bei OpSec ist es besser, zumindest etwas zu tun, als garnichts zu tun.