Schützen Sie Ihr Smartphone

1. Wählen Sie für Ihr Gerät einen Zugangscode mit mindestens sechs Ziffern, verwenden Sie den Fingerabdruck oder die Gesichtserkennung. Wenn also jemand Ihr Smartphone findet oder stiehlt, kann er nicht auf Ihre Daten zugreifen.

2. Sorgen Sie dafür, dass Ihr Smartphone und Ihre Apps stets auf dem neuesten Stand sind. Werden Sie aufgefordert, ein Update vorzunehmen? Tun Sie dies immer so bald wie möglich. Schalten Sie Ihr Smartphone regelmäßig aus. Einige Updates werden bei einem Neustart automatisch installiert.

3. Laden Sie Ihre Apps nur aus den offiziellen App-Stores herunter: aus dem App Store, wenn Sie ein iPhone verwenden, aus dem Google Play Store, wenn Sie ein Gerät einer anderen Marke verwenden.

4. Hüten Sie sich vor gefälschten SMS oder WhatsApp-Mitteilungen. Sie scheinen von einem Unternehmen oder einer Behörde (Bank, Itsme®, Rentendienst, ...) zu stammen oder versprechen Ihnen einen Bonus und fordern Sie auf, auf die darin enthaltenen Links zu klicken, um Ihre Bankcodes zu erhalten, damit Ihre Konten leergeräumt werden können. Seien Sie stets auf der Hut, wenn Sie eine Mitteilung von einer Ihnen unbekannten Nummer erhalten.

5. Nutzen Sie auf Ihrem Gerät ein Antivirenprogramm.

Schützen Sie Ihren Computer

1. Lernen Sie, verdächtige Mails bzw. Mitteilungen zu erkennen. Bei vielen E-Mails, die Sie erhalten, handelt es sich um Betrugsversuche. Überlegen Sie es sich immer zweimal, wenn Sie eine Nachricht von einem Unbekannten erhalten, klicken Sie nie auf einen Link in einer verdächtigen Nachricht.

2. Installieren Sie auf Ihrem Computer ein Antivirenprogramm.

3. Aktualisieren Sie regelmäßig Ihr Betriebssystem und Ihre Programme.

4. Schützen Sie Ihren Computer und Ihre Konten (z. B. E-Mail, Facebook) mit einem langen Passwort, das mindestens 13 Zeichen lang ist. Verwenden Sie unterschiedliche Passwörter.

5. Haben Sie schon von die Zwei-Faktor-Authentisierung (2FA) gehört? Sie ist nicht schwierig und sehr sicher. So werden Ihre wichtigsten Konten doppelt geschützt. Zusätzlich zu Ihrem Passwort verwenden Sie dann einen zweiten Schlüssel, z. B. einen Code, der Ihnen per SMS zugeschickt wird.

Lassen Sie sich am Telefon nicht

1. Sie erhalten einen Anruf von einer unbekannten Nummer? Seien Sie dabei stets auf der Hut.

2. Geben Sie am Telefon niemals persönliche Daten, Passwörter, Kreditkartencodes oder Antwortcodes preis.

3. Rufen Sie niemals eine unbekannte Nummer zurück. Beantworten Sie niemals Anrufe von ausländischen Nummern, die Ihnen unbekannt sind. Rufen Sie auch diese Nummern auf keinen Fall zurück. Wenn Sie jemand braucht, wird er Ihnen eine Nachricht hinterlassen.

4. Glauben Sie nicht alles, was man Ihnen am Telefon erzählt. Microsoft oder andere Technologieanbieter werden Sie niemals anrufen. Auch Ihre Bank wird Sie niemals telefonisch nach Ihren Codes fragen oder Sie auffordern, ein neues Konto anzulegen.

5. Speichern Sie die Nummern der Personen, die Sie kennen. Sperren Sie die Nummern von unerwünschten Anrufern.

Was können Sie noch tun?

Checkliste

✓Ich teile niemals persönliche Informationen, Passwörter, Kreditkartencodes oder Antwortcodes per E-Mail, Telefon, SMS oder über die sozialen Medien mit.

✓Ich lade die Safeonweb-App herunter, um über neue Formen des Online-Betrugs informiert zu werden, und befolge die Ratschläge auf der Website safeonweb.be.

✓Ich sichere mein Smartphone mit einem Zugangscode.

✓Ich richte auf meinem Smartphone und meinem Computer automatische Updates ein.

✓Ich installiere ein Antivirenprogramm auf meinem Smartphone und auf meinem Computer, falls ich nicht bereits eines habe.

✓Ich speichere die Nummern meiner Freunde und Familie in meinem Smartphone. Ich speichere auch die Nummern meiner Bank und anderer Unternehmen, die ich oft kontaktieren muss oder die mich kontaktieren können.

✓Ich schütze mein E-Mail-Postfach mit die Zwei-Faktor-Authentisierung (2FA).

✓Ich schütze auch meine anderen Konten (Facebook, Instagram usw.) mit die Zwei-Faktor-Authentisierung, falls dies möglich ist.

VH : Miguel De Bruycker, Rue de la Loi 18, 1000 Bruxelles

Lassen Sie sich helfen!

Sie wissen nicht, wo Sie mit diesen Tipps anfangen sollen? Sind Sie sich bei einer Nachricht unsicher? Bemerken Sie etwas Seltsames bei Ihrem Computer? Räumen Sie Ihre Zweifel aus! Bitten Sie erfahrenere Freunde oder Familienmitglieder um Hilfe.

Möchten Sie weitere Informationen?
Werfen Sie einen Blick auf www.safeonweb.be und lesen Sie unsere Broschüre „Cyberattacken und Online-Betrug". Laden Sie unsere App Safeonweb herunter, um über die neuesten Bedrohungen informiert zu werden.

Safeonweb

Haben Sie eine verdächtige E-Mail oder Nachricht erhalten?

Senden Sie sie an suspekt@safeonweb.be und löschen Sie sie anschließend. Sie erhalten keine persönliche Antwort auf diese E-Mail. Die in der E-Mail enthaltenen Links werden gesperrt, so dass weniger aufmerksame Internetnutzer nicht mehr auf die Betrüger hereinfallen können.

Kontaktaufnahme

Sind Sie Opfer einer Täuschung oder eines Betrugs geworden?

Melden Sie dies über pointdecontact.belgique.be des FÖD Wirtschaft.
Ihre Nachricht wird in jedem Fall beantwortet. Die zuständigen Stellen werden Ihre Mitteilung analysieren und gegebenenfalls Ermittlungen einleiten.

Zentrum für Cybersicherheit Belgien

Safeonweb ist ein Dienst des Zentrums für Cybersicherheit Belgien.

CENTRE FOR CYBER SECURITY BELGIUM

Safeonweb.be

.be

Betrügern ein Schnippchen schlagen

3 x 5 Tipps für Ihren Schutz

Safeonweb.be