Ransomware

Ihr Computer, Ihre Mobilgeräte oder Ihre digitalen Dateien werden blockiert und es wird ein Lösegeld gefordert, um sie zurückzubekommen.

Was tun?

- Trennen Sie die Verbindung zum Internet (WLAN oder
- Internet-Kabel).
- Trennen Sie ebenfalls sofort alle anderen Geräte, z. B. externe Festplatte oder USB-Stick, vom Computer.
- Wenn Ihr Gerät vollständig blockiert ist und eine Lösegeldforderung gestellt wird, suchen Sie auf www. nomoreransom.org nach dem Schlüssel für diese Ransomware.
- Lassen Sie Ihr Gerät komplett neu installieren und stellen Sie anschließend Ihre Daten mithilfe Ihrer Sicherungskopie wieder her.
- Zahlen Sie nicht: Sie haben keine Gewähr, dass Sie Ihre Daten tatsächlich unversehrt zurückbekommen.

Wie kann ich dies vermeiden?

- Nutzen Sie eine Anti-Ransomware-Software.
- Führen Sie regelmäßig die Updates durch.
- Scannen Sie Ihren Computer regelmäßig

Vorschuss- und Freundschaftsbetrug

Jemand, den Sie kennen oder den Sie im Internet kennen gelernt haben, bittet Sie um Geld.

Was tun?

- Kontaktieren Sie das vorgebliche Familienmitglied oder den Bekannten über einen anderen Kanal, um herauszufinden, ob die Bitte um Hilfe tatsächlich von ihm stammt.
- Überweisen Sie kein Geld jemanden, den Sie online kennen gelernt haben, oder an Familienmitglieder, die „plötzlich" eine andere Kontonummer haben.
- Brechen Sie jeglichen Kontakt mit dem Betrüger ab.

Wie kann ich dies vermeiden?

- Ignorieren Sie Freundschaftsanfragen von Fremden.
- Teilen Sie keine sexuell eindeutigen Fotos oder Videos.

Phishing

Phishing ist Online-Betrug mithilfe gefälschter E-Mails, Websites oder Nachrichten. Cyberkriminelle versuchen dabei, Ihr Vertrauen auszunutzen. Sie versuchen, mit Emotionen wie Lust und Angst zu spielen.

Was tun?

- Wenn Sie ein Passwort preisgegeben haben, das Sie auch anderweitig verwenden, ändern Sie es sofort.
- Wenn Sie auf einen Link klicken, der zu einer Website führt, auf der Sie Ihre Bankdaten angeben müssen, überprüfen Sie zunächst, ob es sich um die echte Website Ihrer Bank handelt. Wenn auch nur der geringste Zweifel besteht, unterlassen Sie jegliche Zahlung.
- Wenn Sie eine Datei heruntergeladen haben, löschen Sie sie und führen Sie einen Antivirenscan durch.

Wie kann ich dies vermeiden?

- Lernen Sie, verdächtige Nachrichten zu erkennen.
- Überlegen Sie zweimal, bevor Sie klicken.
- Laden Sie nur Apps aus einem offiziellen App Store herunter.

Account hack

Ein Account Hack liegt vor, wenn ein Hacker Zugang zu den Anmeldedaten eines Online-Kontos (Account) hat. Der Hacker kann Nachrichten in Ihrem Namen posten oder Ihre Kontakte anschreiben.

Was tun?

- Haben Sie noch Zugang zu diesem Account? Ändern Sie Ihr Passwort (auch bei anderen Konten, in denen Sie dasselbe Passwort verwenden) und informieren Sie Ihre Kontakte.
- Können Sie auf Ihr Account nicht mehr zugreifen? Verwenden Sie die Wiederherstellungsoptionen, um den Zugriff wiederherzustellen, und ändern Sie dann alle Ihre Passwörter.

Wie kann ich dies vermeiden?

- Aktivieren Sie die zweistufige Verifizierung.
- Verwenden Sie für jedes Account ein anderes (sicheres) Passwort und speichern Sie dies in einem Passwort-Safe.
- Teilen Sie Ihre Passwörter niemals anderen Personen mit.

Tech Scam

Sie werden über das Festnetz von jemandem angerufen, der sich als Mitarbeiter eines IT-Unternehmens (Microsoft, Apple, Ihr IT-Provider) ausgibt. Der Betrüger gibt vor, es gäbe ein Sicherheitsproblem mit Ihrem Computer und bietet Ihnen seine Hilfe an.

Wie kann ich dies vermeiden?

- Misstrauen Sie immer Anrufen von Unternehmen, die Sie auffordern, bestimmte Aktionen auf Ihrem Computer vorzunehmen.
- Lassen Sie nie einen Unbekannten, Ihren Computer übernehmen.
- Führen Sie keine Zahlungen aus, solange ein Unbekannter Ihren Computer übernommen hat.

CEO-betrug

Bei einem CEO-Betrug werden Unternehmen von Cyberkriminellen kontaktiert und zu einer Zahlung aufgefordert. Die Cyberkriminellen geben sich als CEO, CFO oder eine vertrauenswürdige Person aus und bitten einen Mitarbeiter des Finanzwesens oder der Buchhaltung, eine dringende Zahlung auszuführen.

Wie kann ich dies vermeiden?

- Informieren Sie Ihre Mitarbeiter entsprechend und warnen Sie sie vor dieser Vorgehensweise.
- Die Buchhaltung verfügt über klare Vorgaben und Anweisungen für Zahlungen.

Sextortion scam

Sie erhalten eine E-Mail, in der Erpresser vorgeben, Ihren Computer gehackt und intime Fotos von Ihnen gemacht zu haben. Die Erpresser drohen damit, die Bilder ins Internet zu stellen, wenn Sie nicht einen bestimmten Betrag zahlen.

Was tun?

- Reagieren Sie nicht auf die
- Zahlungsaufforderung.
- Löschen Sie die Nachricht.
- Markieren Sie die Nachricht als Spam oder unerwünscht.
- Blockieren Sie den Absender.

An wen kann man sich nach einem Cyberangriff oder Online-Betrug wenden?

Polizei

Wenn Sie Geld verloren haben oder erpresst werden, empfehlen wir Ihnen, Anzeige bei der Polizei zu erstatten. Sie können die Anzeige bei Ihrer örtlichen Polizeidienststelle erstatten.

Es ist wichtig, der Polizei so viele Informationen wie möglich vorzulegen. Im Folgenden finden Sie eine Liste der Informationen, die Sie bereits vorab zusammenstellen können:

- Wurde Geld von Ihrem Konto abgebucht? Nehmen Sie die Kontoauszüge mit.
- Sind Sie mit jemandem über die sozialen Medien in Kontakt getreten? Fügen Sie einen Screenshot des Profils des Verdächtigen und einige
- Screenshots der geführten Gespräche bei.
- Haben Sie eine gefälschte Website geöffnet, die beispielsweise der Ihrer Bank oder einer anderen Einrichtung ähnelte? Machen Sie einen Screenshot und bringen Sie ihn zwecks Erstattung Ihrer Anzeige mit.
- Wurden Sie über einen Onlineshop betrogen? Machen Sie einen Screenshot der Werbeanzeige oder des Angebots, auf das Sie geantwortet haben, sowie einen Screenshot vom Profil des Betrügers.
- Haben Sie eine E-Mail von dem Betrüger erhalten? Speichern Sie die Mail ab und drucken Sie sie aus.

Ihre bank und Cardstop

Wenden Sie sich an Ihre Bank und an Cardstop unter 078 170 170, wenn Sie Bankdaten mitgeteilt haben,
wenn Geld von Ihrem Konto verschwindet oder wenn Sie Geld an einen Betrüger überwiesen haben.

So können etwaige illegale Transaktionen noch gestoppt werden.
Wenn Sie einen Betrug melden wollen, können Sie Ihre Bank unter einer speziellen Nummer erreichen: https://beschermjezelfonline.be/bank-contacteren-for-assistance.

Safeonweb

Haben Sie eine verdächtige E-Mail oder Nachricht erhalten?

Senden Sie sie an verdacht@safeonweb.be und löschen Sie sie dann. Sie werden hierauf keine persönliche Antwort erhalten. Die Links in Ihrer E-Mail
werden blockiert, damit weniger aufmerksame Internetnutzer nicht zu Opfern werden. Wenn Sie am Arbeitsplatz eine verdächtige Nachricht erhalten, sollten Sie die dort geltenden Phishing-Bestimmungen befolgen, z. B. die Nachricht an die IT-Abteilung weiterleiten.

Meldestelle

Sind Sie Opfer einer Täuschung oder eines Betrugs geworden?

Dann melden Sie dies über https://meldpunt.belgie.be des FÖD Wirtschaft. Sie erhalten am Ende Ihrer Mitteilung stets eine Empfehlung. Die zuständigen Dienststellen werden Ihre Mitteilung analysieren und gegebenenfalls eine Untersuchung einleiten.

Zentrum für Cybersicherheit Belgien (ZCB)

Wenn Ihr Unternehmen von einem Cyberangriff betroffen oder Opfer einer Ransomwareist und dies melden oder sich vertraulich beraten lassen möchte, können dies bei CERT.be, dem Cyber Emergency Response Team des ZCB unter https://www.cert.be tun.

CENTRE FOR CYBER SECURITY BELGIUM

Safeonweb.be

.be

Cyber-Attacken und Online-Betrug

Worum geht es, was kann ich tun und wie kann ich es verhindern?

Safeonweb.be