

WAS TUN, WENN SIE OPFER EINES CYBERANGRIFFS ODER BETRUGS WERDEN

OFFIZIELLE QUELLE LU-Alert · RTL, 100.7 · 112

DAS TUN SIE JETZT

- 1** Trennen Sie das betroffene Gerät vom Internet: WLAN ausschalten oder Kabel ziehen. Löschen Sie noch nichts; Nachrichten, E-Mails und Bildschirmfotos sind Ihre Beweise.
- 2** Schützen Sie zuerst Ihr Geld. Wenn Sie Kartendaten eingegeben, bezahlt oder Bankcodes weitergegeben haben, rufen Sie sofort Ihre Bank an, und den auf Ihrer Karte genannten Kartenbetreiber (in Luxemburg meist Worldline), um die Karten sperren zu lassen.
- 3** Ändern Sie Ihre Passwörter von einem Gerät, dem Sie vertrauen, zuerst für E-Mail und Bank. Melden Sie jedes Gerät ab, das Sie nicht kennen, und schalten Sie die Anmeldung in zwei Schritten ein.
- 4** Stoppen Sie die Ausbreitung. Sagen Sie Ihren Kontakten, dass Ihr Konto oder Ihre Nummer gehackt wurde, damit sie Nachrichten ignorieren, die scheinbar von Ihnen kommen.
- 5** Melden Sie den Vorfall. Nutzen Sie die nationale Hilfsstelle für Cyberbetrug (cyberfraud.lu), informieren Sie Ihre Bank und erstatten Sie Anzeige bei der Polizei, wenn Geld oder Dokumente gestohlen wurden. Bewahren Sie die Aktenzeichen auf.
- 6** Trauen Sie keiner Nachricht zur Krise, die Geld, Codes oder Dokumente verlangt. Behörden verlangen nie Geld, Spenden laufen nur über vorher angekündigte Kanäle, und Sie geben Ihre Ausweispapiere niemandem, der Hilfe anbietet.
- 7** Wenn jemand in Uniform oder mit Dienstausweis vor Ihrer Tür steht und sich etwas falsch anfühlt, lassen Sie die Tür zu und rufen Sie die Polizei unter **113** an. Betrüger kopieren Uniformen und Abzeichen.

VORHER

KONTEN ABSICHERN

- Verwenden Sie für jedes Konto ein langes, einmaliges Passwort und lassen Sie einen Passwort-Manager sie sich merken. Schalten Sie überall die Anmeldung in zwei Schritten ein, wo es sie gibt, vor allem für E-Mail, Bank und Behördendienste.
- Schalten Sie automatische Updates auf Telefonen, Computern und dem Router ein, und lassen Sie den Virenschutz an. Ändern Sie das Standardpasswort auf jedem neuen Gerät.
- Sperren Sie jedes Gerät mit PIN, Passwort oder Fingerabdruck. Geben Sie Apps nur die Berechtigungen, die sie brauchen.
- Haben Sie mehr als einen Weg, sich bei Ihrer Bank und bei öffentlichen Diensten anzumelden, damit ein verlorenes Telefon oder eine verlorene Karte Sie nicht aussperrt.

- Geben Sie online weniger über sich preis. Adressen, Urlaubsdaten und Fotos von Dokumenten helfen Betrügern, glaubwürdig zu klingen.

SICHERN, WAS SIE NICHT VERLIEREN DÜRFEN

- Kopieren Sie Ihre Fotos, Dokumente und Kontakte auf eine externe Festplatte und lassen Sie sie abgesteckt, wenn Sie sie nicht benutzen. Erneuern Sie die Kopie, wenn Sie Ihren Notvorrat prüfen, **zweimal im Jahr, bei der Zeitumstellung**.
- Bewahren Sie die Nummern, die Sie brauchen würden, auf Papier auf: die Kartensperr-Hotline Ihrer Bank, Ihre Versicherung, Ihren Arzt, die Menschen, die Sie anrufen würden. Legen Sie sie zu Ihrem **Plan**.

DIE ZEICHEN EINES BETRUGS ERKENNEN

- Dringlichkeit, Drohungen, ein Gewinn oder die Aufforderung, zu klicken, zu zahlen oder eine Kopie

Ihres Ausweises zu schicken, sind Warnzeichen. Ebenso Rechtschreibfehler, seltsame Absenderadressen und Webadressen, die der echten fast gleichen.

- Klicken Sie nie auf einen Link in einer unerwarteten Nachricht. Tippen Sie die Adresse selbst ein oder rufen Sie unter einer Nummer zurück, die Sie selbst herausgesucht haben, nicht unter einer aus der Nachricht.
- Offizielle Warnungen erreichen Sie über LU-Alert, das Radio und offizielle Websites, nie über eine Nachricht, die Sie zum Zahlen auffordert. Siehe **Warnungen und Sirenen**.
- Bevor Sie eine Warnung weiterleiten, prüfen Sie, wer sie wann und von wo gepostet hat und ob verlässliche Quellen sie bestätigen. Bilder und Videos können mit KI erzeugt sein.

DANACH

- Beobachten Sie Ihre Kontoauszüge und Konten mehrere Wochen lang, und melden Sie jede Abbuchung, die Sie nicht kennen, sofort.
- Bereinigen Sie das Gerät, bevor Sie es wieder verbinden: Lassen Sie einen vollständigen Virenschutz laufen, oder setzen Sie es zurück und

stellen Sie eine Sicherung von vor dem Angriff wieder her.

- Gehen Sie noch einmal jedes Konto durch: Ändern Sie die Passwörter, die Sie in der Eile übersprungen haben, und prüfen Sie, ob Wiederherstellungs-E-Mail und Telefonnummer noch Ihre sind.

- Wenn ein Arbeitsgerät oder ein Arbeitskonto betroffen war, informieren Sie noch am selben Tag die IT-Ansprechperson bei der Arbeit.
- Sich nach einem Betrug dumm, wütend oder ängstlich zu fühlen, ist häufig. Sprechen Sie mit jemandem, dem Sie vertrauen; das warnt auch die anderen.

WENN SIE ...

MIT KINDERN

- Vereinbaren Sie, dass Kinder nie Passwörter weitergeben, nie online bezahlen und nie Fotos von sich oder von Dokumenten verschicken, ohne Sie vorher zu fragen. BEE SECURE, die nationale Stelle für sicheren Internetgebrauch, hat Material für Familien.

ÄLTER ODER ALLEIN LEBEND

- Vereinbaren Sie eine Familienregel: Niemand, dem Sie wichtig sind, wird Sie je am Telefon oder per Nachricht um Geld, einen Code oder eine Karte bitten. Wenn ein Anrufer sagt, er sei von Ihrer Bank oder der Polizei, legen Sie auf und rufen Sie die Nummer an, die auf Ihrer Karte steht.
- Legen Sie eine Karte mit diesen Regeln neben das Telefon.

WÄHREND EINER GRÖßEREN KRISE

- Wenn Strom oder Netze ausfallen, können Karten und Geldautomaten versagen. Halten Sie Bargeld zu Hause: **€70** pro Erwachsenen und **€30** pro Kind.
- Betrug hat in einer Krise Hochsaison: falsche Sammlungen, falsche Beamte, falsche Hilfsangebote. Prüfen Sie, wer sammelt, und geben Sie nur über Kanäle, die die Behörden angekündigt haben.

KURZ UND EINFACH

 Trennen Sie das gehackte Gerät vom Internet.

 Rufen Sie Ihre Bank an, um Ihre Karten zu sperren.

 Behörden verlangen nie Geld von Ihnen.

 Sagen Sie Ihren Kontakten, dass Ihr Konto gehackt wurde.

 Echte Warnungen kommen von LU-Alert und aus dem Radio, nicht aus einer Nachricht, die Geld verlangt.

Zuletzt geprüft: 25/10/2026 Quellen für diese Seite