

**Mitgliederversammlung
2025**

130
Jahre





ELBA & INFINITY

Raiffeisen Infinity

- ✘ Online Banking für Firmenkunden
- ✘ webbasiert → orts- und zeitunabhängig
- ✘ Flexibel und multibankfähig
- ✘ Sicher durch Zwei Faktor Authentifizierung, Rollen- und Berechtigungssteuerung
- ✘ Zahlreiche Mehrwert Funktionen
 - ✘ Anforderung Bankgarantie
 - ✘ Zentrale Dokumentenablage für pdf-Kontoauszüge
 - ✘ Direkte Beraterkommunikation



- ✘ Umstellungsquote von Elba Business auf Infinity: 93%
- ✘ Ausblick 2025:
 - ✘ Umstellung letzter ELBA Business Kunden mit Funktionen, die im Infinity noch nicht verfügbar sind
 - ✘ Umstellung von MBS auf EBICS
 - ✘ Neue Funktionen wie zum Beispiel neue Druckfunktion, CSV Download,... → Umsetzung konkreter Kundenfeedbacks
 - ✘ Ende und Deaktivierung von ELBA Business mit 1.10.2025

Raiffeisen ELBA

✘ Vorteile

- ✘ Übersichtlichkeit und Benutzerfreundlichkeit
- ✘ Höchste Sicherheitsstandards
- ✘ pushTAN für einfache Freigaben
- ✘ Schnelle und intuitive Bedienung

✘ ELBA in Zahlen

- ✘ 2.178.628 registrierte Nutzer:innen
- ✘ 50.300.068 Logins im Jänner 2025
- ✘ 233.753 Überweisungen täglich





Cyberkriminalität



TLP:GREEN

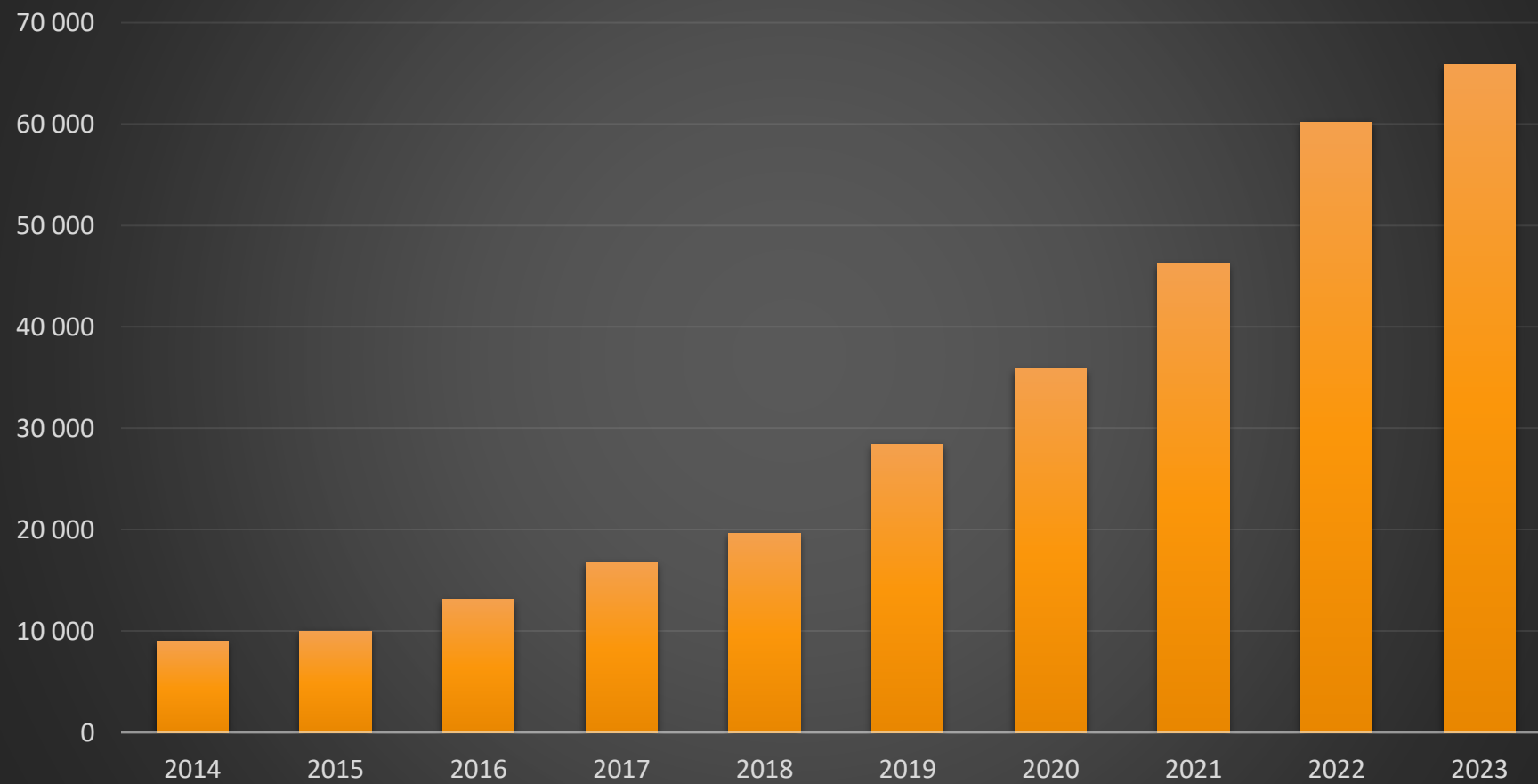
CYBERCRIME

Aktuelle Bedrohungen und Entwicklung

 Bundesministerium
Inneres
Bundeskriminalamt

STATISTIK

Internetkriminalität





Aktuelle Phänomene

Hot Spots

- Online-Investment-Fraud (Cyber-Trading-Fraud, Pig Butchering, etc.)
 - **Starke Verlagerung zu Kryptowährungen**
- Non-delivery Fraud (Fakeshops, Bestellbetrug etc.)
- Business-Email-Compromise (BEC, CEO-Fraud, etc.)
- Cyber-Angriffe (Ransomware, DDOS)
- Account Hacks (Social-Media, Marktplätze, E-Mail, Zahlungsdienste etc.)
- Phishing Attacken (Banking-SMS, Postlieferung, Behörden etc.)
- Cybermobbing (KI-generierte/manipulierte Nacktbilder, etc.)
- Massenerpressung E-Mails (Fake-Behörden Schreiben)
- Kinderpornografie



Aktuelle Phänomene

 Österreichische
Gesundheitskasse

Hallo mein lieber Kunde

Email: [REDACTED]

Sie haben eine ausstehende Rückerstattung im System erkannt, dass Sie zum Erhalt dieser 2

Ihre Rückerstattung ist online möglich: (

Registrationsnummer: 180088684468

Referenz: OGK-AT8055W

Um die schnelle Online-Zahlung zu akzeptieren, speichern Sie die Rückerstattungsdaten

f X YouTube in

Österreichische Gesundheitskasse Wie
ÜBER DIE ÖGK KONTAKT

Von: Österreich.g.v.at <[REDACTED]@online.nl>
Gesendet: Samstag, 6. April 2024 10:42
Betreff: Rückerstattungsnummer 1078629014

15:10

oe24

Nummer der Rückerstattung

Österreichische Regierung

Der letzte Restbetrag Ihres Kontos wird ausgezahlt. Bitte füllen Sie einen Antrag

- Online-Rückerstattung: C
- Rückerstattungsnummer
- Registrierungsdatum: Eir
- Rückerstattungsbetrag: 4

Der Betrag wird innerhalb von 4 W

15:10

oe24

Großer Skandal: ÖGK verweigert Komm...
Mitarbeiter Christo

Während der Live-Übertragung „Willkommen“

HAT DAS SYSTEM BEF...
€ 115.347,...

JETZT TEILNEHMEN

Guten Tag, mein fre...
kam Zu unserer Ken...
sowohl ihre Karriere...
Ihr lebenslauf von m...
Online-Personalverr...
favorisiert wurden. d...
wir, Es wäre Toll Ihre...
Nebenbeschäftigung...
Sie Während Ihrer F...
Durchführen können...
sind Leicht Wie eine...
ihre meinung Über il...
ab. ★★★★★ K...
Der zeit - sie entsch...
Sie Diese bewertung...

☀️ das tagesspesen liegt zwischen 300
Und 1.000 euro und wird am gleichen
Tag zur Verfügung gestellt 💰💰💰
sollten sie Interesse Haben, treten sie
bitte via WhatsApp mit uns In Kontakt:
[+447961461432](https://wa.me/447961461432)

Berühren und halten, um zu reagieren

13:43

<

+43 67

SMS-
Heu

Hallo mama/papa, me...
funktioniert nicht mel...
ist meine neue numm...
mir ein nachtricht abe...
app+436767395420

13:01

5G

HelloSMS >

Textnachricht • SMS
Heute, 11:24

Ihr Paket wurde zurückge-
sandt, da die Hausnummer im
Paket fehlt. Bitte aktualisieren
Sie die Versandinformatio-
nen: <http://postataustria.cc/at>

Anzeige idio lillybeauty41 • C



Aktuelle Phänomene



Datenlecks & Phishingangriffe

MACHEN WIR
PHISHEN
IMPOSSIBLE!

Phishing bedeutet Datendiebstahl. Mit Phishing-Nachrichten versuchen Betrüger, an Passwörter, Bankdaten oder andere sensible Informationen zu gelangen. Hier erfährst du, wie du deine persönlichen Daten schützen kannst.

MEHR ERFAHREN

Eine Initiative von Österreichischen Banken PSA Bundesministerium Inneres
in Kooperation mit Watchlist Internet

- <https://www.phishen-impossible.at/>
- Die 4 häufigsten Phishing-Attacken
 - Online-Banking
 - Tech Support
 - Paketdienst
 - Finanzamt

Phishing-Regeln – so machst du Phishen impossible



Achte auf Nachrichten, die dich zum dringenden Handeln auffordern:

Traue keiner Nachricht oder Mail, die sensible Daten verlangt. Vor allem, wenn dringlich erscheint, mit Konsequenzen droht oder Belohnung verspricht.



Prüfe genau, an wen du Geld überweist.

Prüfe die URL auf eine sichere HTTPS-Verbindung und korrekte Rechtschreibung. Online-Shops sollten auch ein SSL-Zertifikat, ein vollständiges Impressum und Gütesiegel wie "Trusted Shops" aufweisen.



Prüfe immer Absender und Links, bevor du klickst.

Für die Weitergabe deiner persönlichen Daten gilt: im Zweifelsfall Nein. Klicke nur, wenn du absolut sicher bist, dass der Absender seriös ist. Antivirus-Programme und Zwei-Faktor-Authentifizierung bieten zusätzlichen Schutz.



Öffne keine Anhänge von unbekannten Absendern.

Klicke bei verdächtigen E-Mails immer auf den Absender, um zu prüfen, ob die Adresse echt ist, und achte auf korrekte Logos und Schreibweisen. Kontaktiere das Unternehmen im Zweifelsfall direkt, um die Echtheit zu bestätigen.



Wurden meine Zugangsdaten gestohlen??

<https://haveibeenpwned.com/>

';--have i been pwned?

Check if your email address is in a data breach

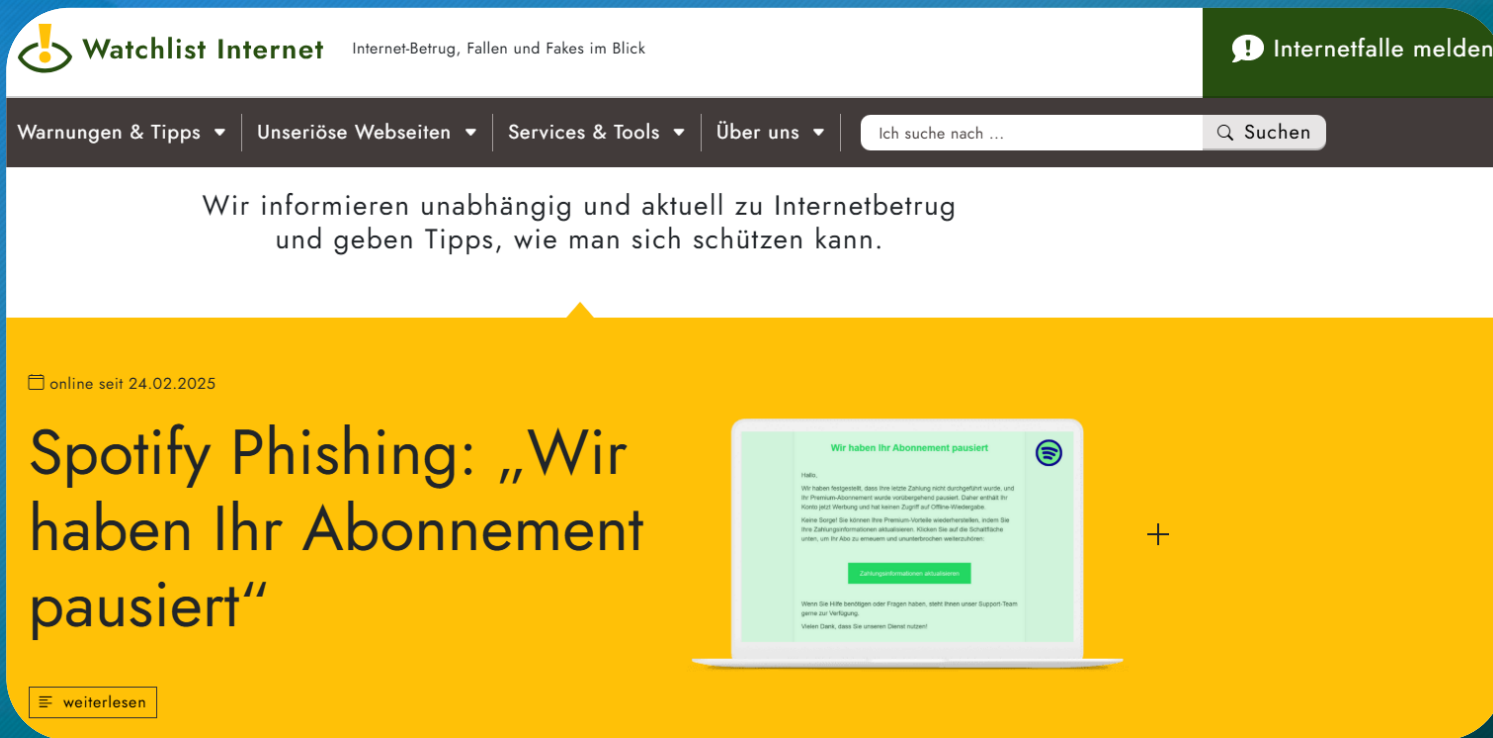
email address

pwned?

14 Milliarden betroffene Zugangsdaten und Konten

Watchlist-Internet

<https://www.watchlist-internet.at/>



- Aktuelle Warnungen
- Newsletter / Apps / Channels
- Fakeshop – Detector
- Awareness Playbooks
- Webinare
- Erklärvideos
- Meldefunktion

Weiterführende Informationen

- Watchlist Internet
 - www.watchlist-internet.at
- Phishen Impossible!
 - <https://www.phishen-impossible.at/>
- SaferInternet
 - <https://www.saferinternet.at/>
- IKT-Sicherheitsportal
 - <https://www.onlinesicherheit.gv.at/>
- BK-C4 Meldestelle für Internetkriminalität
 - <https://bundeskriminalamt.at/306/start.aspx>
 - against-cybercrime@bmi.gv.at

Vielen Dank

5 Grundregeln im Internet

1

Seien Sie misstrauisch!

Hinter Versprechungen und verlockenden Angeboten stecken meist betrügerische Absichten.

2

Schützen Sie Computer und Handy!

Halten Sie Ihre Geräte, Systeme und Programme wie z.B. Betriebssystem, Firewall immer auf aktuellem Stand.

3

Sichern Sie Ihre Datenübertragung!

Verwenden Sie verschlüsselte Internetseiten. Sie erkennen diese an einem Schloss-Zeichen in der Adressleiste. Meiden Sie öffentliches WLAN.

4

Wählen Sie sichere Passwörter!

Wählen Sie lange Passwörter mit Sonderzeichen und Zahlen oder verwenden Sie Passwortmanager. Halten Sie Ihre Passwörter geheim.

5

Sichern Sie regelmäßig Ihre Daten!

Wichtige Daten sollten Sie mittels Backup-Software auf externe Festplatten oder Datenträgern sichern. Trennen Sie diese danach vom System.

**VIELEN DANK
FÜR DIE AUFMERKSAMKEIT!**

130
Jahre

**Raiffeisen
Region Wiener Alpen**

