

# Die **Zentrale Ansprechstelle Cybercrime** informiert zu Betrugsmaschen mit manipulierten Rechnungen und Zahlungsaufforderungen

01011010  
01000001  
01000011



# Achtung vor Betrugsmaschen mit manipulierten Rechnungen und Zahlungsaufforderungen

Die Zentrale Ansprechstelle Cybercrime des Landeskriminalamt Schleswig-Holstein (ZAC) warnt vor einem Anstieg an Betrugsfällen mit manipulierten Rechnungen und Zahlungsaufforderungen.

Durch sogenannte BEC-Scams (Business-E-Mail Compromise) sind in letzter Zeit Sportvereine verstärkt betroffen.

## Betrugsmethoden:

- **Gefälschte Zahlungsanweisungen:**  
Vereinsmitglieder erhalten vermeintliche E-Mails von Vorstandsmitgliedern mit dringenden Überweisungsaufforderungen. Dabei geben die Täter manipulierte Bankverbindungen an.
- **Manipulierte Rechnungen:**  
Bereits erbrachte Leistungen werden abgerechnet, aber die Kontodaten im Anhang durch die Täter geändert.
- **E-Mail-Adressen-Manipulation:**  
Die Täter nutzen entweder gehackte Vereins-Mailadressen oder erstellen täuschend ähnliche Adressen, um Zahlungsaufforderungen zu senden.

## Schutzmaßnahmen:

- **Prüfung der Absenderadresse:**  
Überprüfen Sie sorgfältig die vollständige E-Mail-Adresse des Absenders. Achten Sie auf minimale Abweichungen (z. B. zusätzliche Buchstaben oder Domainnamen).
- **Für Vereine und Rechnungssteller:**
  - Verwenden Sie individuelle, nichtöffentliche E-Mail-Adressen für Rechnungsversand.
  - Überprüfen Sie regelmäßig die Einstellungen und Filter in Ihren E-Mail-Konten auf Manipulation.
  - Nutzen Sie verschlüsselte und signierte E-Mails, um Betrug zu erschweren.
  - Ändern Sie Passwörter regelmäßig und verwenden Sie Zwei-Faktor-Authentifizierung.
- **Für Mitglieder und Empfänger:**
  - Überprüfen Sie die Kontodaten einer Rechnung sorgfältig und vergleichen Sie sie mit den bekannten Bankverbindungen.
  - Seien Sie bei ausländischen Bankverbindungen besonders wachsam.
  - Verifizieren Sie Aufforderungen durch einen telefonischen Rückruf bei den offiziellen Vereinskontakten.
  - Kontaktieren Sie bei einem Betrugsverdacht sofort die Polizei und versuchen Sie, bereits ausgeführte Überweisungen zu stoppen.

## Handeln Sie umsichtig und informieren Sie alle relevanten Mitglieder Ihres Vereins.

Weitere Informationen erhalten Sie bei der [Zentralen Ansprechstelle Cybercrime Schleswig-Holstein](#).

Die ZAC ist erste Anlaufstelle für Unternehmen, Behörden und sonstige Institutionen in Schleswig-Holstein rund um das Thema Cybercrime.

Hier stehen **werktags** von **08:00 Uhr bis 18:00 Uhr** und **samstags** von **08:00 Uhr bis 13:00 Uhr** unter der **Hotline +49 431 160-42727** kompetente Mitarbeitende für Fragen und Antworten, sowie etwaige Sachverhaltsaufnahmen zur Verfügung.

**Herausgeber**

Ministerium für Inneres, Kommunales  
Wohnen und Sport  
des Landes Schleswig-Holstein  
Landeskriminalamt,  
Zentrale Ansprechstelle Cybercrime  
Mühlenweg 166, 24116 Kiel  
[cybercrime@polizei.landsh.de](mailto:cybercrime@polizei.landsh.de)  
Telefon 0431 160-42727

**Grafik/Layout**

Landespolizei Schleswig-Holstein, StSt 4

**Bilder**

Landespolizeiamt Schleswig-Holstein

**Die Landespolizei im Internet**

[www.polizei.schleswig-holstein.de](http://www.polizei.schleswig-holstein.de)

Nachdruck und sonstige Vervielfältigung -  
auch auszugsweise - nur mit Quellenangabe gestattet.

Februar 2025