

# Die Zentrale Ansprechstelle Cybercrime

## informiert zu Betrugstaten zum Nachteil von Ämtern und Behörden in Schleswig-Holstein



# Dringende Warnung vor Betrugstaten zum Nachteil von Ämtern und Behörden in Schleswig-Holstein

Die Zentrale Ansprechstelle Cybercrime (ZAC) des LKA Schleswig-Holstein möchte Sie über eine derzeit akute Bedrohungslage informieren: Tätergruppen haben sich gezielt auf sog. BEC-Scams (Business-E-Mail-Compromise) zum Nachteil von Ämtern und Behörden spezialisiert.

## Hintergrund der Betrugsmasche:

Tätergruppen werten gezielt öffentliche Ausschreibungen aus und nehmen anschließend im Namen der ausschreibenden Stelle Kontakt mit der Gewinnerfirma auf. Dabei wird um die nochmalige Übersendung einer Rechnung gebeten.

Erfolgt diese Übermittlung, haben die Täter eine originale Rechnung in Händen, die nun manipuliert wird. Im Anschluss wird die gefälschte Rechnung mit geänderten Bankdaten im Namen des tatsächlichen Gewinners der Ausschreibung an das Amt oder die Behörde gesandt.

Diese Masche tritt bundesweit auf, auch in Schleswig-Holstein sind bereits mehrere Fälle bekannt. Die Schadenssummen bewegen sich dabei häufig im sechsstelligen Bereich.

## Schutzmaßnahmen:

### 1. Prüfung der Absenderadresse:

- Überprüfen Sie die vollständige E-Mail-Adresse des Absenders sorgfältig. Achten Sie auf Abweichungen wie leicht veränderte Domainnamen oder ungewöhnliche Schreibweisen.
- Seien Sie besonders wachsam, wenn Ihnen die E-Mail-Adresse unbekannt ist oder keinen direkten Bezug zur bekannten Person oder Firma hat.

### 2. Verifizierung von Rechnungen:

- Telefonische Bestätigung: Fordern Sie eine telefonische Bestätigung beim vermeintlichen Rechnungssteller ein, bevor Zahlungen angewiesen werden. Nutzen Sie hierfür ausschließlich offiziell bekannte Rufnummern.
- Bestätigung per E-Mail: Fordern Sie eine Bestätigung per E-Mail ein, aber antworten Sie nicht direkt auf die verdächtige Nachricht. Verwenden Sie stattdessen eine offiziell bekannte E-Mail-Adresse des Rechnungsstellers.
- Kontodaten prüfen: Vergleichen Sie die angegebenen Bankverbindungen mit den bereits bekannten Daten des Unternehmens. Seien Sie besonders vorsichtig bei ausländischen Bankkonten.

### 3. Sicherer Rechnungsversand

- Verwenden Sie verschlüsselte und signierte E-Mails, um die Manipulation von Rechnungen zu erschweren.

### 4. Maßnahmen bei Betugsverdacht

- Wenn Sie einen Betugsverdacht haben oder bereits betroffen sind, kontaktieren Sie sofort die Polizei.
- Versuchen Sie, bereits ausgeführte Überweisungen bei Ihrer Bank rückgängig zu machen.

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 Sachverhaltaufnahmen 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