igs
psychiatrie. sozial.

PHISHING-MAILS | Schütze dich mit dem 10-Sekunden-Check

Auch die igs Bern wird immer wieder Ziel von Phishing-Mails und Betrugsversuchen. Mit dem **10-Sekunden-Check in drei Schritten** kannst du dich gezielt davor schützen.

1. ABSENDERTRICK: Überprüfe Mailadresse von Absender:innen

Mail-Betrüger:innen benutzen oft Namen, die du kennst. Beispiele: «IT-Support», «Microsoft» oder eben «igsbern»).

- **Das solltest du tun:** Klicke oder tippe auf den Namen der Absenderin oder des Absenders und überprüfe, ob die E-Mail-Adresse echt ist. Mail-Adressen der igs Bern enden immer auf *@igsbern.ch*, jene des RCB auf *@recoverycollegebern.ch*.
- **Beispiel:** Ist hinter dem Namen eine eigenartige Mailadresse versteckt (z.B. *info.igsbern@service-x12.com* statt *info@igsbern.ch*)? Dann lösche das Mail sofort!

2. LINK-VORSCHAU: Überprüfe verdächtige Links

Verdächtige Links führen oft auf gefälschte Anmeldeseiten, die dein Passwort stehlen wollen.

- **Das solltest du tun:** Fahre am PC mit der Maus über den Link, ohne zu klicken (Hover). Unten links im Browser siehst du das echte Ziel.
- **Beispiel:** Steht im Link-Text z.B. *www.igsbern.ch/login*, aber die Link-Vorschau zeigt eine völlig andere Webadresse (z.B. *bit.ly/blabla*)? Dann Finger weg von diesem Link!

3. KÜNSTLICHER ZEITDRUCK: Werde hellhörig bei Fristen und Drohungen

Phishing will, dass du dein Gehirn ausschaltest.

- **Das solltest du tun:** Werde misstrauisch bei Mails, die dir eine Frist setzen, dir drohen oder dir grossen Druck machen. Suche nach gefälschten Mailadressen oder Links. Im Zweifelsfall löschst du das Mail oder fragst bei der IT (urs.gilgen@igsbern.ch) nach.
- **Beispiele:** «Ihr Account wird in 4 Stunden gesperrt!»; «Probleme mit Ihrer Gehaltsabrechnung – sofort prüfen!»; «Paketzustellung fehlgeschlagen, hier Porto nachzahlen»

Betrugsversuche: weitere typische Beispiele

Typ	Masche	Dein Schutz
Die IT-Falle	Mail mit der Info: «Dein Postfach ist voll. Klicke hier für mehr Speicher.» (Sobald du auf den Link klickst, wirst du nach deinem Passwort gefragt)	Lösche das Mail. Die igs Bern fragt dich **nie** nach deinem Passwort.
Die Chef-Masche	Mail von deiner vorgesetzten Person: «Bist du gerade erreichbar? Ich brauche dringend Hilfe bei einer Zahlung/Gutscheinkauf.»	Überprüfe, ob die Mail-Adresse echt ist. Im Zweifelsfall rufst du die Person kurz an und fragst nach.
Das Dokument	Mail mit der Info: «Anbei die neuen Richtlinien zur Hygiene.» (Anhang ist ein .zip oder .exe)	Öffne nie Anhänge von Absender:innen, die du nicht kennst, oder die du nicht erwartet hast – besonders wenn sie auf .exe oder .zip enden.

Was tun, wenn es trotzdem passiert ist?

Jede:r kann auf Phishing-Versuche reinfallen. Wenn dir das passiert, dann gehe wie folgt vor:

1. **Informiere sofort die IT** (urs.gilgen@igsbern.ch)
2. **Ändere dein Passwort** von einem anderen Gerät aus, falls du es preisgegeben hast

KURZ-CHECK: Erst denken, dann klicken!

1. **Ist die Absender-Adresse echt?** @igsbern.ch? @recoverycollegebern.ch?
2. **Ist das Link-Ziel verdächtig?** Maus drüberhalten und überprüfen
3. **Macht das Mail Stress?** Tief durchatmen und IT fragen

igs Bern | 22. Januar 2026