Aktuelle Cybercrime-Begriffe, die du kennen solltest

Stand: Mai 2026. Für Awareness-Schulungen, Phishing-Analysen und Unterricht sind aktuell besonders Begriffe rund um **Phishing, KI-Betrug, Ransomware, Identitätsmissbrauch und Lieferkettenangriffe** relevant. In der Schweiz nennt das BACS für das zweite Halbjahr 2025 besonders Phishing, SMS-Blaster, Ransomware, Business-E-Mail-Compromise und Software-Lieferketten als wichtige Entwicklungen. (ncsc.admin.ch)

1 Besonders aktuelle Begriffe

Begriff	Kurz erklärt	Typisches Beispiel
Phishing	Betrügerische Nachricht, die Zugangsdaten, Kreditkartendaten oder Zahlungen abgreifen will.	Gefälschte Mail von „ChatGPT“, „Post“, „Microsoft“ oder „Bank“.
Spear Phishing	Gezielt personalisiertes Phishing gegen einzelne Personen oder Rollen.	Mail an Buchhaltung mit echtem Namen, korrekter Funktion und passendem Kontext.
Whaling	Spear Phishing gegen Führungskräfte.	Angriff auf CEO, CFO, Schulleitung oder Verwaltungsleitung.
Smishing	Phishing per SMS.	„Ihr Paket konnte nicht zugestellt werden. Bezahlen Sie CHF 1.99.“
Vishing	Phishing per Telefon oder Sprachanruf.	Angeblicher Bankmitarbeiter fordert Sicherheitscode.
Quishing	Phishing über QR-Codes.	Mail oder Plakat mit QR-Code, der auf eine gefälschte Login-Seite führt. Das BACS erwähnt ausdrücklich auch QR-Codes als Phishing-Methode. (ncsc.admin.ch)
Real-Time-Phishing	Angreifer fangen Zugangsdaten und MFA-Codes in Echtzeit ab.	Opfer gibt Login und SMS-Code ein; Angreifer meldet sich parallel sofort an.
Double Phishing	Nach einem erfolgreichen Phishing wird das Opfer nochmals kontaktiert und weiter geschädigt.	Nach gefälschter Zahlungsseite folgt ein Telefonanruf durch angeblichen Support.
SMS-Blaster	Gerät, das sich als Mobilfunkantenne ausgibt und betrügerische SMS lokal verteilt.	Fake-SMS im Umkreis von etwa einem Kilometer. In der Schweiz seit Sommer 2025 beobachtet. (ncsc.admin.ch)
BEC / Business E-Mail Compromise	Kompromittierung oder Täuschung im geschäftlichen E-Mail-Verkehr.	Angreifer ändern Bankdaten auf Rechnungen. Das BACS meldete 73 Fälle im zweiten Halbjahr 2025. (KMU.admin)
CEO-Fraud	Betrug im Namen einer Führungsperson.	„Bitte überweise sofort, vertraulich, keine Rückfragen.“

Begriff	Kurz erklärt	Typisches Beispiel
Deepfake Fraud	Betrug mit künstlich erzeugten Stimmen, Bildern oder Videos.	Gefälschter Videoanruf mit angeblicher Führungsperson.
Voice Cloning	KI-gestützte Nachahmung einer Stimme.	Angeblicher Angehöriger oder Vorgesetzter ruft an und fordert Geld.
AI-Phishing	Mit KI erzeugte Phishing-Texte, oft sprachlich sauber und personalisiert.	Keine Rechtschreibfehler mehr, überzeugender Ton, passende Details.
Prompt Injection	Manipulation eines KI-Systems durch versteckte oder direkte Anweisungen.	Eine Webseite enthält Text, der einen KI-Assistenten zu falschen Aktionen verleiten soll.
Data Poisoning	Manipulation von Trainings- oder Wissensdaten.	Falsche Daten werden in ein System eingeschleust, damit spätere Ausgaben verfälscht werden.
Ransomware	Schadsoftware verschlüsselt Daten oder Systeme und fordert Lösegeld.	Schule, KMU oder Gemeinde kann nicht mehr arbeiten.
Double Extortion	Kombination aus Verschlüsselung und Datendiebstahl.	„Zahle, sonst veröffentlichen wir eure Daten.“
Triple Extortion	Zusätzlich werden Kundschaft, Partner oder Medien unter Druck gesetzt.	Angreifer schreiben auch betroffene Dritte direkt an.
Ransomware-as-a-Service / RaaS	Mietmodell für Ransomware-Infrastruktur.	Technische Anbieter stellen Plattform, Partner führen Angriffe aus.
Initial Access Broker / IAB	Kriminelle verkaufen gestohlene Zugänge zu Firmen.	VPN-Login oder RDP-Zugang wird im Untergrund verkauft.
Infostealer	Malware, die Passwörter, Cookies, Wallets oder Browserdaten stiehlt.	Gestohlene Session-Cookies ermöglichen Login ohne Passwort.
Credential Stuffing	Automatisiertes Ausprobieren geleakter Passwörter bei anderen Diensten.	Ein altes Passwort aus Datenleck funktioniert auch bei Microsoft 365.
Password Spraying	Wenige häufige Passwörter werden gegen viele Konten getestet.	„Sommer2026!“ gegen hunderte Benutzerkonten.
MFA Fatigue / Push Bombing	Opfer wird mit MFA-Anfragen bombardiert, bis es versehentlich bestätigt.	Viele Login-Bestätigungen auf dem Smartphone.
Session Hijacking	Übernahme einer aktiven Sitzung, oft über gestohlene Cookies.	Angreifer nutzt bestehende Login-Session ohne Passwort.
Malvertising	Schädliche Werbung in Suchmaschinen oder Werbenetzwerken.	Gefälschte Support- oder Login-Seite als Suchmaschinenanzeige.

Begriff	Kurz erklärt	Typisches Beispiel
SEO Poisoning	Manipulierte Suchtreffer führen auf Schadseiten.	Suche nach „Teams Download“ führt zu Fake-Installer.
Supply-Chain-Angriff	Angriff über Software, Dienstleister, Updates oder Bibliotheken.	Kompromittiertes Open-Source-Paket wird in viele Anwendungen eingebaut. BACS erwähnt entsprechende Angriffe auf Open-Source-Komponenten. (ncsc.admin.ch)
Zero-Day	Ausgenutzte Sicherheitslücke, bevor ein Patch verfügbar ist.	Neue Schwachstelle in VPN, Firewall oder Browser wird sofort angegriffen.
Living off the Land	Angreifer missbrauchen vorhandene Systemwerkzeuge statt eigener Malware.	PowerShell, WMI, Remote-Tools oder Admin-Werkzeuge werden zweckentfremdet.
DDoS	Überlastungsangriff gegen Websites oder Dienste.	Website einer Behörde oder Schule ist nicht erreichbar.
ORB-Netzwerke	Verdeckte Netzwerke aus kompromittierten Routern und IoT-Geräten.	Private Router werden als Infrastruktur für Angriffe missbraucht. Das BACS nennt ORB-Netzwerke ausdrücklich als Entwicklung in der Schweiz. (ncsc.admin.ch)
Cybercrime-as-a-Service / CaaS	Kriminelle Dienstleistungen werden modular verkauft.	Phishing-Kits, Malware, Hosting, gestohlene Logins, Geldwäscherei.
Money Mule / Finanzagent	Person, die Geld für Kriminelle weiterleitet.	„Nebenjob“: Geld empfangen und gegen Provision weiterüberweisen.

2 Die wichtigsten Begriffe für Nicht-Techniker

Für eine kompakte Awareness-Folie würde ich diese **10 Begriffe** priorisieren:

1. Phishing
2. Smishing
3. Vishing
4. Quishing
5. Business E-Mail Compromise
6. CEO-Fraud
7. Deepfake Fraud
8. Ransomware
9. MFA Fatigue
10. Infostealer

3 Kurze Einordnung

Die gefährlichste Entwicklung ist nicht ein einzelner neuer Angriff, sondern die **Kombination**: Eine KI-generierte Mail wirkt glaubwürdig, ein QR-Code umgeht einfache Linkkontrollen, ein Echtzeit-Phishing-Proxy fängt MFA-Codes ab, und gestohlene Zugangsdaten werden später für BEC oder Ransomware genutzt. ENISA beschreibt das aktuelle Bedrohungsbild entsprechend als stark geprägt durch Phishing, technische Ausnutzung von Schwachstellen, Malware und wiederverwendete Angriffswerkzeuge. (enisa.europa.eu)

Für die Schweiz sind derzeit besonders praxisrelevant: **Phishing in Schweizer Kontexten**, **SMS-Blaster**, **Ransomware gegen Organisationen**, **BEC im Rechnungswesen** und **Angriffe über Software-Lieferketten**. (ncsc.admin.ch)

4 Wo KI bei einer unsicheren Mail mit Zahlungsaufforderung helfen kann

KI kann dich vor allem bei der **Ersteinschätzung** unterstützen. Sie ersetzt aber nicht die Prüfung über offizielle Kanäle, deine Bank, deinen IT-Support oder den angeblichen Anbieter.

1. Inhalt der Mail beurteilen

KI kann den Text auf typische Betrugsmerkmale prüfen:

Merkmal	Worauf KI achten kann
Zeitdruck	„innert 24 Stunden“, „letzte Mahnung“, „Konto wird gelöscht“
Drohung	Sperrung, Inkasso, Löschung, Strafanzeige
Unklare Forderung	keine Rechnungsnummer, kein Vertrag, keine konkrete Leistung
Ungewöhnliche Zahlung	neue IBAN, Kryptowährung, Gutscheinkarten, ausländisches Konto
Sprachliche Auffälligkeiten	unpassender Ton, schlechte Übersetzung, falsche Anrede
Verdächtige Links	Linktext sieht seriös aus, Zieladresse aber nicht
Gefälschter Absender	angezeigter Name passt nicht zur echten Mailadresse

Das BACS warnt allgemein davor, bei verdächtigen Mails Links zu öffnen, Anhänge auszuführen oder Zugangsdaten beziehungsweise Zahlungsdaten einzugeben. Verdächtige Phishing-Mails können an reports@antiphishing.ch weitergeleitet oder über das BACS gemeldet werden. (ncsc.admin.ch)

2. Linkziele und Absender plausibilisieren

Du kannst der KI zeigen:

- den sichtbaren Absender
- die tatsächliche Absenderadresse
- den Betreff

- den Mailtext
- sichtbare Links
- Angaben zu Betrag, IBAN, Zahlungsfrist und Anbieter

Die KI kann dann prüfen, ob diese Angaben zusammenpassen.

Beispiel:

Frage	Nutzen
Passt die Domain zur angeblichen Firma?	Erkennt gefälschte Absender oder Login-Seiten
Ist die IBAN plausibel?	Hilft bei Auffälligkeiten wie Auslandskonto oder Namensabweichung
Ist der Ton typisch für Betrug?	Erkennt Druck, Drohung, künstliche Dringlichkeit
Wird ein Anhang unnötig wichtig gemacht?	Warnsignal bei ZIP-, HTML-, EXE- oder Makro-Dateien

3. Zahlungsaufforderung sachlich einordnen

KI kann dir helfen, aus der Mail eine Prüfliste zu machen:

Prüffrage	Bedeutung
Habe ich bei diesem Anbieter wirklich ein Konto?	Grundprüfung
Erwarte ich eine Rechnung?	Plausibilität
Stimmt der Betrag mit Vertrag oder Bestellung überein?	Zahlungsprüfung
Stimmt die Kundennummer?	Identitätsprüfung
Stimmt die IBAN mit früheren Rechnungen überein?	Betrugsprüfung
Wurde eine neue Bankverbindung genannt?	starkes Warnsignal
Gibt es eine echte Rechnung im Kundenportal?	verlässlicher als Mail-Link

Gerade bei gefälschten Rechnungen oder geänderten Bankverbindungen empfiehlt sich die Kontrolle über einen **separaten Kanal**: also nicht auf die Mail antworten, sondern die bekannte Telefonnummer, die offizielle Website oder das bestehende Kundenportal verwenden.

4. Technische Hinweise aus Headern erklären

Wenn du die vollständigen Mailheader hast, kann KI helfen, diese verständlich zu interpretieren:

Header-Element	Was KI erklären kann
Return-Path	wohin unzustellbare Mails zurückgehen
Received	über welche Server die Mail lief
SPF	ob der sendende Server erlaubt war
DKIM	ob die Mail kryptografisch signiert wurde
DMARC	ob die Domain Schutzregeln verletzt
Reply-To	ob Antworten an eine andere Adresse umgeleitet werden

Wichtig: Eine saubere Header-Prüfung ist ein starkes Indiz, aber keine absolute Garantie. Auch echte Systeme können Fehlkonfigurationen haben, und gute Phishing-Mails können technisch sauber wirken.

5. Eine sichere Antwort formulieren

KI kann dir helfen, eine neutrale Rückfrage zu formulieren, ohne sensible Daten preiszugeben.

Beispiel:

Guten Tag

Ich habe eine Zahlungsaufforderung erhalten, kann diese aber nicht eindeutig zuordnen. Bitte senden Sie mir die Rechnung mit Rechnungsnummer, Leistungsdatum, Vertragsgrundlage und offizieller Bankverbindung nochmals zu. Aus Sicherheitsgründen öffne ich keine Links aus Zahlungsaufforderungen per E-Mail.

Freundliche Grüsse

Noch besser: Nicht direkt auf die verdächtige Mail antworten, sondern eine **bekannte offizielle Kontaktadresse** verwenden.

6. Was du der KI nicht geben solltest

Bei der Prüfung durch KI solltest du vertrauliche Daten vorher entfernen oder anonymisieren.

Nicht ungeprüft eingeben	Besser so
Kreditkartennummer	**** **** **** 1234
vollständige IBAN	nur Land und letzte 4 Stellen
Passwort / MFA-Code	niemals eingeben
Kundennummer	teilweise schwärzen
Personendaten Dritter	anonymisieren
vertrauliche Verträge	nur relevante Ausschnitte

7. Was KI nicht entscheiden sollte

KI kann Hinweise liefern, aber nicht verbindlich entscheiden:

Entscheidung	Zuständig
Zahlung auslösen	du / Buchhaltung / Verantwortliche Person
Konto sperren oder Karte blockieren	Bank / Kartenanbieter
Strafanzeige	Polizei
IT-Sicherheitsvorfall	IT-Support / Sicherheitsverantwortliche
rechtliche Beurteilung	Fachperson / Rechtsberatung

Falls bereits Geld überwiesen wurde oder Zugangsdaten eingegeben wurden, ist rasches Handeln wichtig: Bank kontaktieren, Karte sperren, Passwörter ändern, Sitzungen abmelden und den Vorfall melden. Das BACS verweist bei finanziellen Schäden auf eine Strafanzeige bei der örtlichen Polizei. (ncsc.admin.ch)

Geeigneter KI-Prompt

Du kannst der KI zum Beispiel schreiben:

Prüfe diese Mail auf mögliche Phishing- oder Betrugsmerkmale.

Beurteile Absender, Betreff, Sprache, Zahlungsaufforderung, Links, Anhänge, Fristen, IBAN und Druckmittel.

- Erstelle eine Risikoeinschätzung in den Stufen niedrig, mittel, hoch.
- Gib mir eine Prüfliste, was ich vor einer Zahlung kontrollieren muss.

Ich habe persönliche Daten anonymisiert.

Kurzfazit

KI hilft dir bei:

- Betrugsmerkmale erkennen
- Mailtext einordnen
- Links und Absender plausibilisieren
- Header verständlich machen
- Prüflisten erstellen
- sichere Rückfragen formulieren
- Aber: Nie direkt aus einer unsicheren Mail bezahlen. Keine Links anklicken. Keine Zugangsdaten eingeben. Immer über offizielle Kanäle prüfen.

KI-Tools wie chatGPT personalisieren

Wenn man sicher gehen will, dass ein KI-Tool nicht lügt und fantasiert, gewisse Schreibregeln einhält und möglichst nur konkrete Ansätze und Antworten liefert, ist eine Personalisierung (meisten im entsprechenden Einstellungsbereich verfügbar) unerlässlich.

Beispiel

Antworten auf Deutsch (Schweizer Rechtschreibung, immer «ss» statt «ß»). Persönliche Du-Ansprache. Präzise, fachlich korrekt, praxisnah. **Keine erfundenen Inhalte oder Spekulationen. Bei fehlenden Angaben gezielt nachfragen. Bei komplexen Themen Quellen oder nachvollziehbare Herleitungen angeben.**

Texte klar strukturieren mit Titeln, Listen und Tabellen. Keine HTML-Formatierungen in normalen Antworten. Tabellen direkt für Word/Excel nutzbar aufbauen. Fachbegriffe für Einsteiger erklären. Redundanzen und Floskeln vermeiden.

Bilder:

- sprachlich korrekt
- immer «ss» statt «ß»
- gut lesbare Schrift
- moderne Gestaltung
- keine abgeschnittenen Texte

Word mit «Formatvorlagennamen.dotm» (sollte vorgängig hochgeladen werden):

- Hauptthema → «Titel»
- «Tipps & Tricks» usw. → «Zwischentitel»
- übrige Titel → «Untertitel»
- Nummerierung → «1. NumAufz»
- Aufzählungen → «PunktAufz»
- Tastenkürzel fett + kursiv
- saubere Seitenumbrüche
- einheitliche Formatierung

HTML aus hochgeladenen Dokumenten:

- H1 → H3 (13 pt, fett)
- Untertitel → H4 (12 pt, fett)
- Zelladressen fett
- Tabellen/Farben wie Original
- keine Kopf-/Fusszeilen
- farbige Inhalte als kontrastierte Rahmen
- originale Aufzählungssymbole übernehmen

Zusätzlich:

- Excel-Formeln deutsch & Microsoft-365-kompatibel
- Schweizer Tastenkürzel
- DSGVO/Schweizer DSG beachten
- keine Gendersternchen/Binnen-I, immer Gender-:

Mit dieser Personalisierung erhält man mehrheitlich sehr gute Ergebnisse.