Formation Prevention

LEITFADEN FÜR DIE RICHTIGEN REFLEXE

Den Fallen des Alltags vorbeugen

12 Themen, die Handgriffe, die Ihr Unternehmen schützen. Am besten griffbereit halten.



BEVOR SIE BEGINNEN

Drei Reflexe, die überall gelten

1

Halten Sie inne

Dringlichkeit, Angst oder eine zu schöne Belohnung sind die liebsten Hebel von Betrügern. Gerade eine drängende Anfrage verdient, dass man langsamer wird.

2

Prüfen Sie über einen anderen Kanal

Rufen Sie die Person oder das Unternehmen unter der Nummer zurück, die Sie bereits kennen, nie unter der in der Nachricht angegebenen.

3

Melden Sie es sofort

Dem IT-Dienst oder Ihrer vorgesetzten Person, auch bei blossem Zweifel und auch wenn Sie schon geklickt haben.

Dieser Leitfaden fasst die 12 Module von Formation Prevention zusammen. Er ersetzt die Module nicht: Er ruft sie Ihnen in Erinnerung, Thema für Thema.

THEMA 01 / 12

Phishing

> Eine manipulierte E-Mail, SMS oder ein QR-Code wirkt in allem, was Sie sehen, echt: Absendername, Logo, Ton. Was sie verrät, ist verborgen.

Schauen Sie auf die echte Adresse

Der angezeigte Name ist frei wählbar. Lesen Sie die ganze Absenderadresse und zeigen Sie mit der Maus auf einen Link (lang drücken auf dem Telefon), um sein echtes Ziel zu sehen.

Misstrauen Sie der Dringlichkeit

Paket zurückgehalten, Konto gesperrt, unbezahlte Rechnung: Eine sehr kurze Frist ist ein Warnsignal, kein Grund, schnell zu handeln.

Tippen Sie die Adresse selbst ein

Um sich bei Ihrer Bank oder einem Dienst anzumelden, geben Sie die Adresse ein, die Sie kennen, statt dem erhaltenen Link zu folgen.

QR-Codes

Scannen Sie keinen QR-Code, der auf einer Parkuhr klebt oder per Post kam, ohne die Adresse zu prüfen, die er öffnet.

MERKEN SIE SICH

Verdächtige Nachricht: nicht klicken, nicht antworten, nicht weiterleiten. Melden Sie sie dem IT-Dienst oder an reports@antiphishing.ch.

THEMA 02 / 12

Identitätsmissbrauch

> Ein falscher Direktor, Lieferant oder Treuhänder verlangt eine dringende, vertrauliche Überweisung oder eine Änderung der Bankverbindung.

- **Rufen Sie unter der bekannten Nummer zurück**

  Kontaktieren Sie die Person über eine Nummer, die Sie bereits hatten, nie über die in der Nachricht oder im Anruf genannte.

- **Halten Sie sich an das Verfahren**

  Eine ungewöhnliche Zahlung durchläuft die vorgesehene doppelte Kontrolle, auch wenn der «Direktor» Geheimhaltung verlangt.

- **Änderung der IBAN**

  Jede Anfrage, die Bankverbindung eines Lieferanten zu ändern, wird telefonisch geprüft, bevor sie erfasst wird.

- **Lesen Sie die Domain**

  Ein einziger abweichender Buchstabe in der Adresse des Absenders genügt dem Betrüger.

MERKEN SIE SICH

Dringlichkeit, Geheimhaltung und Zahlung zusammen: Halten Sie an und prüfen Sie. Niemand wird es Ihnen vorwerfen.

THEMA 03 / 12

Passwörter

> Ein kurzes oder mehrfach verwendetes Passwort ist schnell geknackt und öffnet dann alle Konten, die es verwenden.

- **Zuerst die Länge**

  Mindestens 12 Zeichen, besser 16 oder mehr. Ein leicht zu merkender Satz ist besser als ein kompliziertes Wort.

- **Ein Passwort pro Konto**

  Werden einer Website die Daten gestohlen, bleiben Ihre anderen Konten geschützt.

- **Ein Passwort-Manager**

  Er erstellt und merkt sich starke Passwörter für Sie: der von Ihrem Unternehmen bereitgestellte, oder zum Beispiel Bitwarden oder Proton Pass.

- **Nichts Persönliches**

  Weder Vorname noch Geburtsdatum, Firmenname oder Jahreszahl: Das sind die ersten Versuche eines Angreifers.

MERKEN SIE SICH

Nur ein Passwort müssen Sie sich wirklich merken: das des Managers. Machen Sie es lang und einzigartig.

THEMA 04 / 12

Zwei-Faktor-Authentifizierung

> Mit einem zweiten Faktor genügt ein gestohlenes Passwort nicht mehr, um in Ihr Konto zu gelangen.

- **Überall aktivieren**

  E-Mail, Passwort-Manager, berufliche Konten: überall, wo sie angeboten wird.

- **Eine App bevorzugen**

  Eine Authentifizierungs-App oder ein Sicherheitsschlüssel schützt besser als ein per SMS erhaltener Code.

- **Nie einen Code weitergeben**

  Weder der IT-Dienst noch eine Bank wird Sie danach fragen, weder am Telefon noch per Nachricht.

- **Ablehnen, was Sie nicht angefordert haben**

  Wiederholte Anmeldeanfragen bedeuten, dass jemand Ihr Passwort hat: ablehnen, Passwort ändern und den IT-Dienst informieren.

MERKEN SIE SICH

Bewahren Sie Ihre Wiederherstellungscodes im Passwort-Manager auf, nicht in einer E-Mail.

THEMA 05 / 12

Surfen im Internet

> Eine gefälschte Website kann genau wie die echte aussehen, Schloss-Symbol inbegriffen.

Das Schloss genügt nicht

Es verschlüsselt die Verbindung, sagt aber nichts über die Ehrlichkeit der Website. Lesen Sie die vollständige Adresse.

Vorsicht bei Anzeigen

In den Suchergebnissen können gesponserte Links von Betrügern bezahlt sein: Tippen Sie lieber die offizielle Adresse ein.

Offizielle Downloads

Installieren Sie ein Programm nur von der Website des Herstellers, oder fragen Sie den IT-Dienst.

Falsche Warnungen

Eine Virenwarnung mit Countdown oder einer Nummer zum Anrufen ist eine Falle: Schliessen Sie den Tab. Eine Zertifikatswarnung wird nie ignoriert.

MERKEN SIE SICH

Im Zweifel über eine Seite: schliessen und über die Adresse gehen, die Sie kennen.

THEMA 06 / 12

Öffentliches WLAN

> Im Café, am Bahnhof oder im Hotel kann sich jemand als das offizielle Netz ausgeben und sehen, was Sie senden.

- **Zuerst Ihr Telefon**

  Der Hotspot Ihres Telefons ist sicherer als ein offenes Netz.

- **Das VPN des Unternehmens**

  Aktivieren Sie es, bevor Sie in einem Netz arbeiten, das Sie nicht kontrollieren.

- **Keine heiklen Vorgänge**

  Vermeiden Sie E-Banking und vertrauliche Daten in einem öffentlichen Netz.

- **Manipulierte Anmeldeseiten**

  Eine Seite, die für den WLAN-Zugang eine Kreditkarte oder die Installation eines Programms verlangt: ablehnen. Vergessen Sie das Netz nach der Nutzung.

MERKEN SIE SICH

Ein an der Theke ausgehängtes Passwort macht ein geteiltes Netz nicht zu einem privaten.

THEMA 07 / 12

Ransomware

> Ransomware verschlüsselt die Dateien des Unternehmens und verlangt ein Lösegeld. Sie gelangt oft über einen manipulierten Anhang hinein.

- **Inhalt nicht aktivieren**

  Ein per E-Mail erhaltenes Dokument, das zur Anzeige «Inhalt aktivieren» verlangt, ist ein Warnsignal.

- **Bildschirm gesperrt oder Dateien umbenannt**

  Trennen Sie sofort die Netzwerkverbindung (Kabel und WLAN) und informieren Sie dann den IT-Dienst und Ihre vorgesetzte Person.

- **Nicht bezahlen**

  Und keinen Kontakt zu den Angreifern: Zahlen garantiert weder die Rückgabe der Dateien noch, dass die Daten nicht veröffentlicht werden.

- **Das Backup nicht anschliessen**

  Die Backup-Festplatte würde ebenfalls verschlüsselt. Lassen Sie den IT-Dienst über das weitere Vorgehen entscheiden.

MERKEN SIE SICH

Netz trennen, dann Alarm schlagen: zwei Handgriffe, in dieser Reihenfolge.

THEMA 08 / 12

USB-Sticks und Datenträger

> Ein gefundener oder geschenkter USB-Stick kann Schadsoftware enthalten oder sich sogar als Tastatur ausgeben, die Befehle eintippt.

- **Nie ein unbekannter Stick**

  Ein gefundener, per Post erhaltener oder an einer Messe verschenkter Stick wird nicht angeschlossen: Geben Sie ihn dem IT-Dienst.

- **Verschlüsselte Sticks**

  Verwenden Sie für berufliche Daten die verschlüsselten Datenträger des Unternehmens, keinen privaten Stick.

- **Löschen ist nicht vernichten**

  Dateien löschen oder schnell formatieren entfernt sie nicht wirklich: Übergeben Sie alte Datenträger dem IT-Dienst.

- **Verlorener Datenträger**

  Ein verlorener Stick oder eine verlorene Festplatte mit Unternehmensdaten wird sofort gemeldet.

MERKEN SIE SICH

Sie haben einen zweifelhaften Datenträger angeschlossen: ausstecken, Netz trennen und melden.

THEMA 09 / 12

Homeoffice

> Zu Hause sind der Internet-Router und der Arbeitscomputer Ihr erster Schutz.

- **Richten Sie Ihren Router ein**

  Ändern Sie das ursprüngliche Administratorpasswort, wählen Sie WPA3 (mindestens WPA2) und ein WLAN-Passwort mit mindestens 16 Zeichen, besser 20.

- **Ein Gästenetz**

  Für Besuch und vernetzte Geräte, getrennt von Ihrem Arbeitscomputer.

- **Ein Computer für die Arbeit**

  Nur für die Arbeit genutzt, aktuell gehalten und gesperrt, sobald Sie aufstehen. Zugriff auf Daten über das VPN des Unternehmens.

- **Diskretion**

  Vertrauliche Gespräche und Bildschirm vor fremden Blicken geschützt, Dokumente weggeräumt.

MERKEN SIE SICH

Computer verloren oder gestohlen: Informieren Sie sofort den IT-Dienst.

THEMA 10 / 12

Deepfake und Vishing

> Eine Stimme lässt sich aus wenigen Sekunden Aufnahme nachahmen, ein Gesicht in der Videokonferenz ebenso, und die angezeigte Nummer kann gefälscht sein.

- **Auflegen und zurückrufen**

  Unter der Nummer, die Sie kennen, auch wenn es die Stimme Ihres Direktors ist.

- **Nie ein Code am Telefon**

  Kein Passwort, kein per SMS erhaltener Code, keine PIN, egal wer anruft.

- **Keine Fernsteuerung**

  Installieren Sie kein Programm und lassen Sie keine unbekannte Person (falscher Support, falsche Polizei) Ihren Computer steuern.

- **Das Verhalten zählt mehr als das Aussehen**

  Ungewöhnliche Anfrage, Druck, Geheimhaltung: Auf diese Zeichen sollten Sie hören.

MERKEN SIE SICH

Ein Zweifel während eines Anrufs: Beenden Sie das Gespräch. Der echte Anrufer wird es verstehen.

THEMA 11 / 12

Backups und sensible Dateien

> Defekt, Brand, Ransomware: Ohne aktuelles und sicher aufbewahrtes Backup ist die Arbeit verloren.

- **Die 3-2-1-Regel**

  Drei Kopien der Daten, auf zwei verschiedenen Datenträgern, davon eine an einem anderen Ort (Empfehlung des BACS).

- **Eine Offline-Kopie**

  Trennen Sie die Festplatte nach jedem Backup und testen Sie regelmässig die Wiederherstellung.

- **Mit Mass teilen**

  Eine sensible Datei wird nur mit den betroffenen Personen geteilt, nie über einen Link, der allen offensteht.

- **Falscher Empfänger**

  Ein an die falsche Person gesendetes Dokument wird sofort gemeldet: Das Unternehmen kann gesetzliche Pflichten haben.

MERKEN SIE SICH

Ein Backup, das nie wiederhergestellt wurde, ist nur eine Hoffnung.

THEMA 12 / 12

Meldung von Vorfällen

> Jede Minute zählt: Je früher das Unternehmen Bescheid weiss, desto früher wird der Angriff gestoppt.

- **Sofort**

  Melden Sie es, sobald Sie einen Zweifel haben, auch bei einem knapp vermiedenen Vorfall.

- **Am besten per Telefon**

  Ihr E-Mail-Postfach ist vielleicht schon in falschen Händen.

- **Sagen Sie das Wesentliche**

  Die Uhrzeit, was passiert ist, das betroffene Konto oder die Nachricht und was Sie bereits getan haben.

- **Nichts löschen**

  Und nichts verharmlosen: Das sind wertvolle Hinweise für den IT-Dienst.

MERKEN SIE SICH

Schnell zu melden ist nie ein Fehler.

BEI EINEM VORFALL

Die fünf Handgriffe

1. **Stoppen**
   Nichts mehr anklicken. Bei Verschlüsselung: Netzwerk trennen.
2. **Sofort anrufen**
   Den IT-Dienst und Ihre vorgesetzte Person.
3. **Genau beschreiben**
   Was, wann, welches Konto, welche Nachricht.
4. **Nichts löschen**
   Beweise aufbewahren, kein Kontakt mit Angreifern.
5. **Anweisungen folgen**
   Der IT-Dienst weiss, was zu tun ist.

IHRE KONTAKTE

IT-Dienst _____

Vorgesetzte Person _____

Notfallnummer _____

IN DER SCHWEIZ

Phishing melden
reports@antiphishing.ch

Bundesamt für Cybersicherheit (BACS)
www.bacs.admin.ch

Finanzieller Schaden
Ihre Kantonspolizei

Formation Prevention

FORMATION PREVENTION

Lernen durch Erleben

Module von etwa 10 Minuten, realistische Simulationen und Schweizer Beispiele, damit die richtigen Reflexe zur Gewohnheit werden.

formation-prevention.ch

IMPRESSUM

Datalys
Grand Rue 8
1196 Gland
Schweiz

© 2026 Datalys