RUNDGANG IN BILDERN · ETWA FÜNF MINUTEN

So sieht die Phishing-Simulation aus

Was Ihre Mitarbeitenden im Postfach sehen, wo sie klicken, wie sie melden und was danach bei Ihnen ankommt. Zum Durchgehen mit der Geschäftsleitung, dem Betriebsrat oder der IT — ohne dass vorher eine einzige Übungs-Mail verschickt werden muss.

Die Simulation ist ab Hugo Learn Standard enthalten · auf Deutsch · in Deutschland verarbeitet.

AUF EINEN BLICK

Eine Übungs-Mail, zwei mögliche Wege

Jede Person bekommt eine Mail, die wie ein echter Betrugsversuch aussieht. Danach gibt es genau zwei Wege, und keiner davon hat Folgen für die Person.

Die Mail kommt an

Im normalen Postfach, zwischen der übrigen Post. Von außen ist sie nicht als Übung markiert.

Weg 1: Die Person meldet

Ein Klick auf „Phishing melden“. Das ist das Ergebnis, das Sie sich wünschen, und es zählt in die Melderate.

Weg 2: Die Person klickt

Statt eines Schadens erscheint eine Seite, die erklärt, woran die Mail zu erkennen war. Dazu kommt eine kurze Auffrischung.

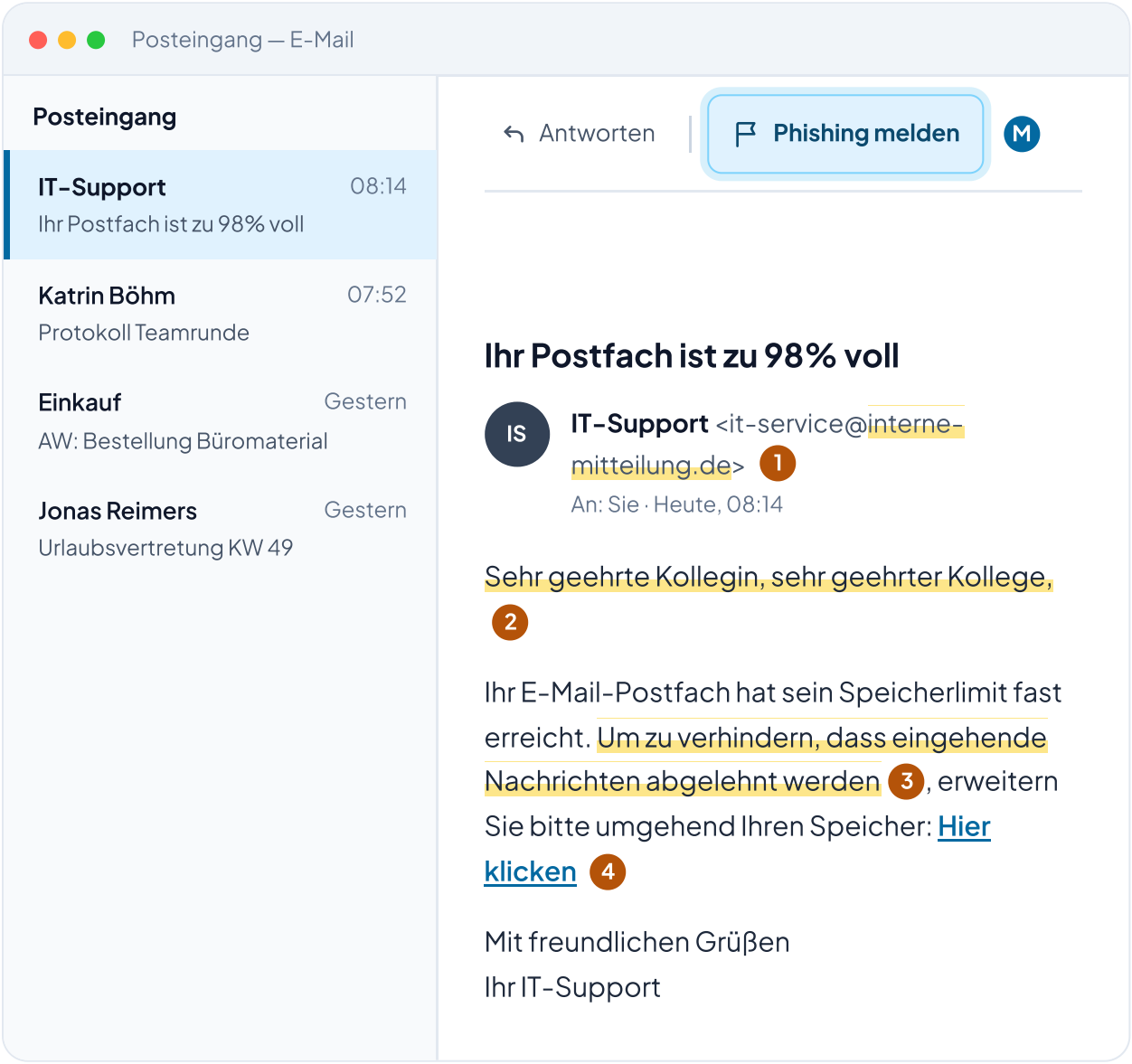
1 DIE MAIL IM POSTFACH

So kommt die Übung bei Ihren Mitarbeitenden an

Hier eine Vorlage der Stufe „leicht“: angeblich schreibt der IT-Support, das Postfach sei fast voll. Sie wählen aus der Bibliothek, was zu Ihrem Betrieb passt — Paketdienst, Gehaltsabrechnung, Schichtplan, Rechnung.

Nachbildung — kein Screenshot

Übungs-Mail in Outlook. Der Wortlaut stammt aus der Vorlagenbibliothek.



Woran man diese Mail erkennt

1 **Absenderadresse prüfen**
Der Name sagt „IT-Support“, die Adresse gehört aber nicht zu Ihrer Firma. Der Blick gehört hinter das @.

2 **Allgemeine Anrede ohne Namen**
Die eigene IT kennt die Person, der sie schreibt.

3 **Druck durch drohenden Datenverlust**
„Nachrichten werden abgelehnt“ soll das Nachdenken abkürzen.

4 **Aufforderung zur Aktion über einen Link**
Speicher erweitert die IT selbst — niemand muss dafür auf einen Link klicken.

M **Der Meldeknopf**
„Phishing melden“ steht in der Leiste über jeder geöffneten Mail. Wo genau, hängt von der Outlook-Version ab.

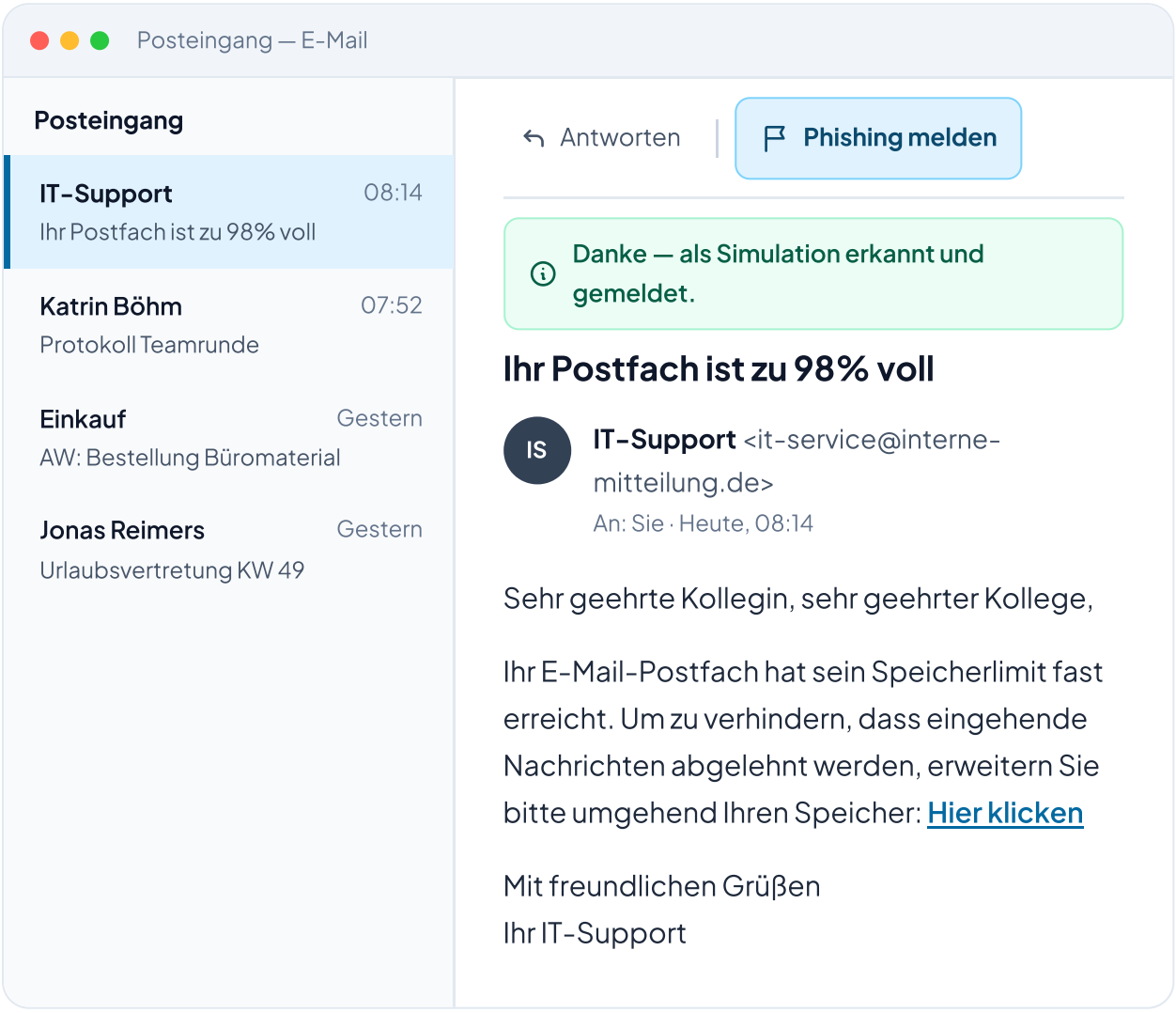
2 WEG 1 · MELDEN

Ein Klick, und die Meldung ist raus

Wer die Mail verdächtig findet, drückt auf „Phishing melden“. Der Knopf erkennt selbst, ob es eine Übung war, und antwortet sofort.

Nachbildung — kein Screenshot

Übungs-Mail in Outlook. Der Wortlaut stammt aus der Vorlagenbibliothek.



War es eine Übung

Die Person liest „Danke — als Simulation erkannt und gemeldet.“ Die Meldung zählt für sie und für die Melderate des Unternehmens.

War es eine echte Verdachts-Mail

Derselbe Knopf leitet sie an die Sicherheits-Adresse Ihres Unternehmens weiter. Die Person liest „Danke für Ihre Meldung — sie wurde an die IT-Sicherheit weitergeleitet.“ So wird aus der Übung eine Gewohnheit für den Ernstfall.

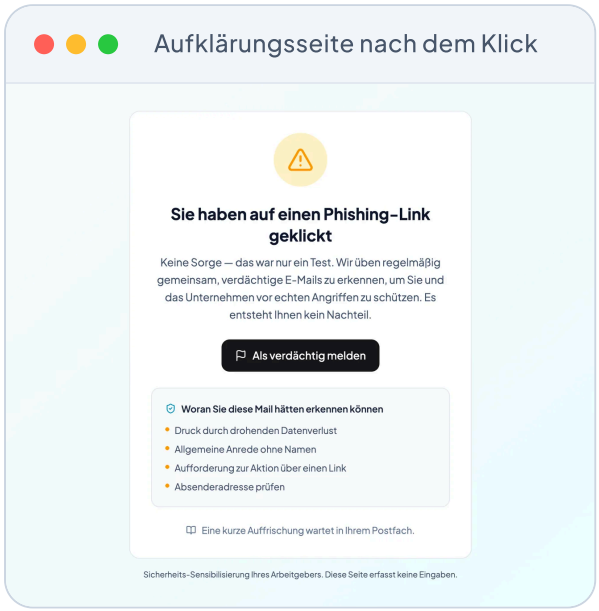
Ohne Knopf: das Melde-Postfach

Wer kein Add-in verteilen möchte oder einen Exchange Server im eigenen Haus betreibt, richtet eine Melde-Adresse ein. Verdächtige Mails werden dorthin weitergeleitet und der Übung automatisch zugeordnet.

3 WEG 2 · GEKLICKT

Wer klickt, lernt sofort — und wird nicht vorgeführt

Der Link führt auf eine Aufklärungsseite. Sie sagt in ruhigem Ton, dass es eine Übung war, zeigt die Warnsignale genau dieser Mail und lässt die Person die Mail nachträglich melden. Eine Anmeldung braucht es nicht, die Seite erfasst keine Eingaben.



Screenshot

Direkt nach dem Klick: die Warnsignale der Mail aus Kapitel 1.



Screenshot

Nachträglich gemeldet: Auch nach einem Klick zählt die Meldung.

Kurze Auffrischung per Mail

Wenige Minuten später liegt eine Lektion von rund vier Minuten im Postfach, passend zum Thema der Mail. Wer das nicht möchte, schaltet sie je Kampagne ab.

Kein Nachteil für die Person

Ein Klick hat keine arbeitsrechtlichen Folgen. Wer Angst vor Folgen hat, meldet einen echten Angriff später, nicht früher.

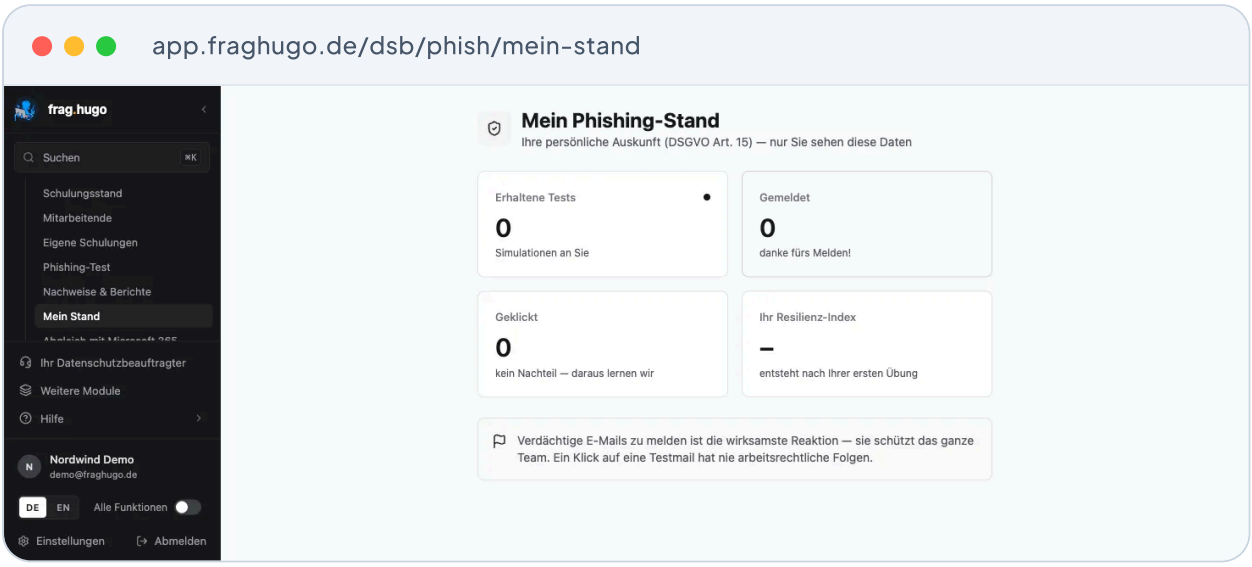
In der Sprache der Person

Die Aufklärungsseite gibt es auf Deutsch und Englisch, je nachdem, was für die Person eingestellt ist.

4 DER EIGENE STAND

Jede Person sieht ihre Zahlen — und nur sie

Unter „Mein Stand“ steht, wie viele Übungen jemand bekommen, gemeldet und angeklickt hat. Das ist zugleich die persönliche Auskunft nach Art. 15 DSGVO. Vorgesetzte haben auf diese Ansicht keinen Zugriff.

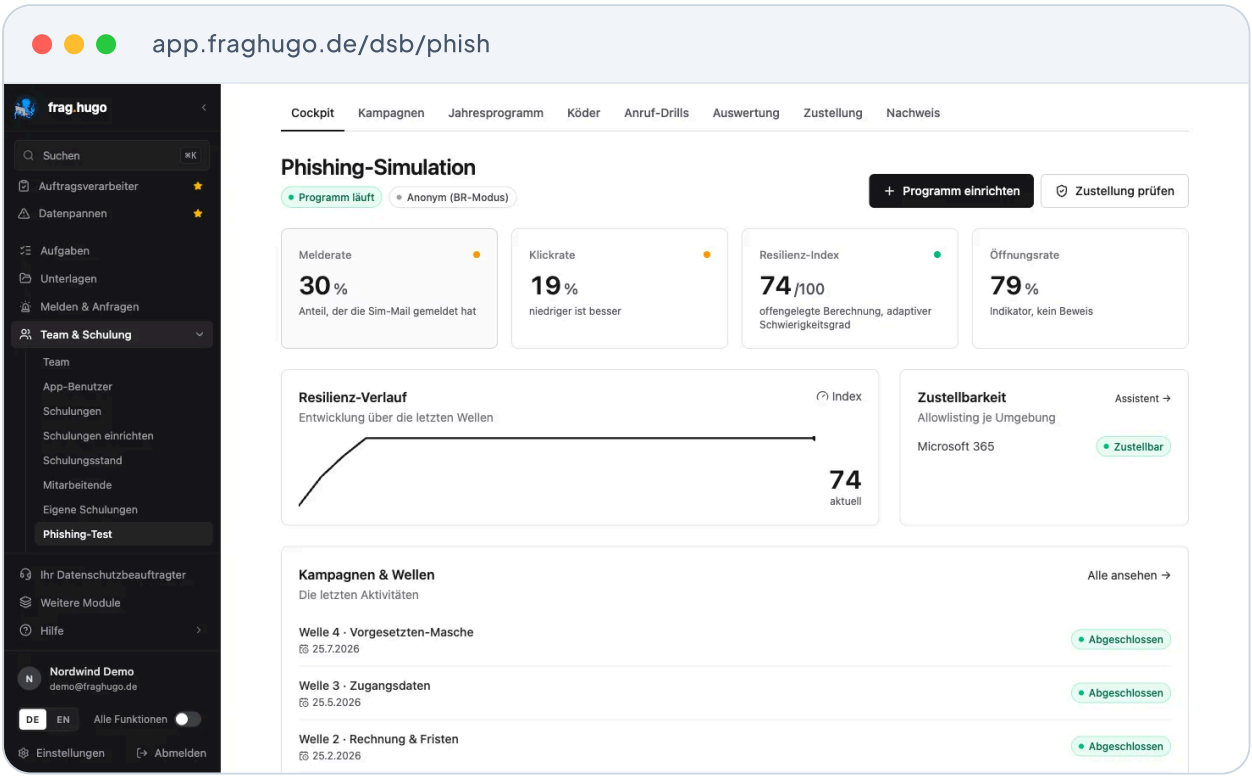


Screenshot Ansicht einer Person vor ihrer ersten Übung.

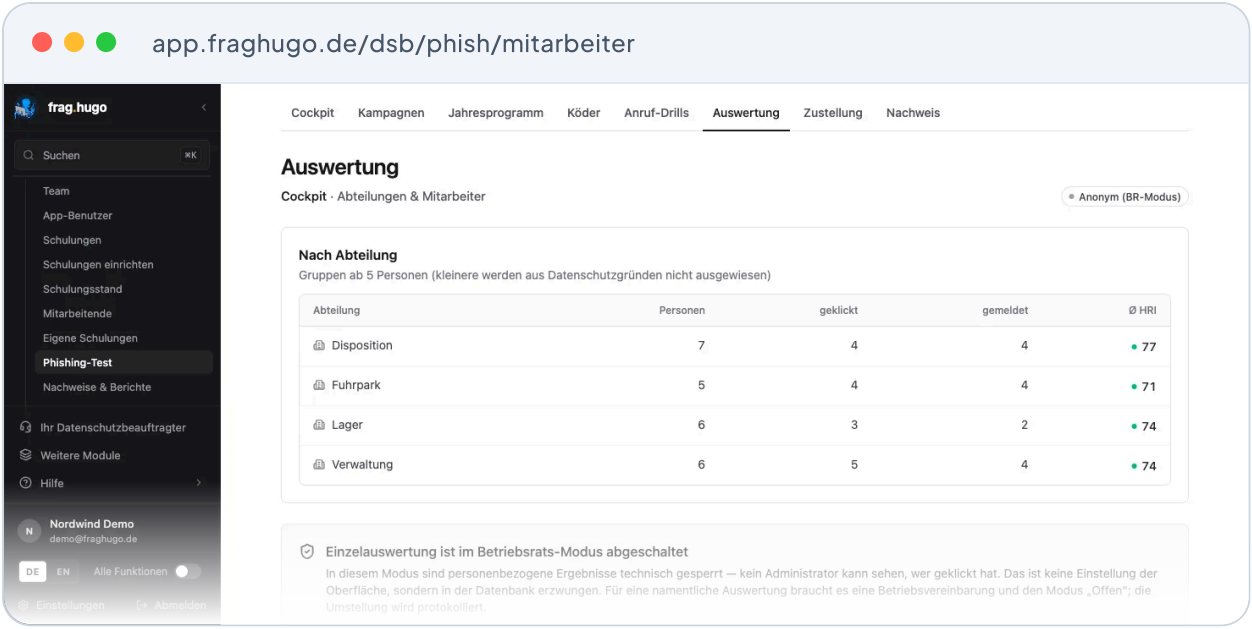
5 DIE AUSWERTUNG

Was bei der Geschäftsleitung ankommt

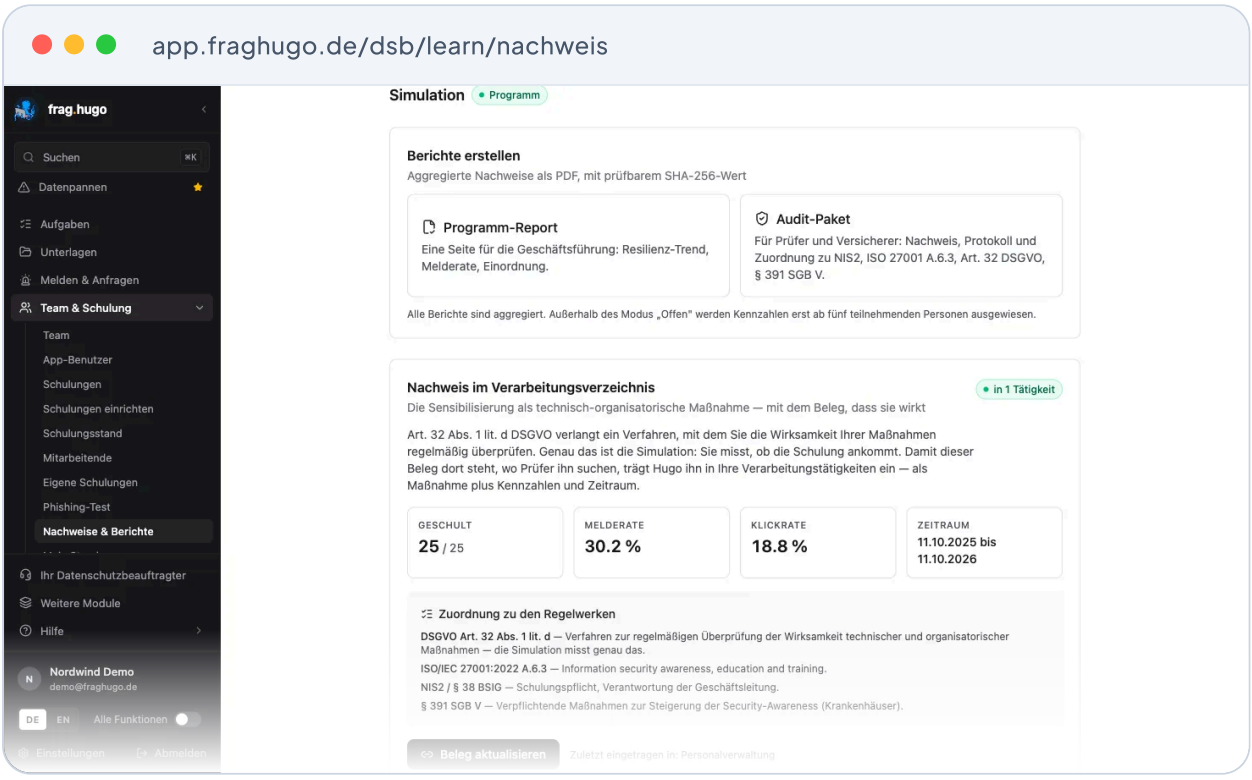
Zwei Zahlen zählen: wie viele geklickt haben und wie viele gemeldet haben. Die zweite ist die wichtigere, denn sie sagt, ob im Ernstfall jemand Alarm schlägt. Namen stehen nirgends. Die Zahlen in den Bildern stammen aus unserem Vorführ-Mandanten.



Screenshot Das Cockpit: Melderate, Klickrate und der Verlauf über die Wellen.



Screenshot Nach Abteilung, erst ab fünf Personen. Wer geklickt hat, sieht niemand.



Screenshot Der Bericht als PDF — für Prüfer, Versicherung und Betriebsrat.

6 DIE EINRICHTUNG

Was Ihre IT einmalig einrichtet

Auf den Rechnern wird nichts installiert. Die Übungs-Mails kommen auf dem normalen Mailweg an; damit der Mailfilter sie durchlässt, braucht es eine einmalige Freigabe. Solange die nicht bestätigt ist, verschickt die Plattform keine Übung.

1

Zustellung freigeben

Ihre IT trägt Absender-Domain, Sende-Adresse und Übungs-Adresse einmal in den Mailfilter ein, damit die Übungs-Mails nicht in der Quarantäne landen. Für Microsoft 365 geht das mit einem Knopf in der Plattform. Rechnen Sie mit rund einer halben Stunde.

Anleitung Zustellbarkeit → (https://docs.fraghugo.de/hugo-phish/zustellbarkeit/)

2

Meldeweg wählen

Mit Microsoft 365 verteilt Ihre IT den Knopf „Phishing melden“ zentral an alle Postfächer. Ohne Add-in richten Sie ein Melde-Postfach ein, an das verdächtige Mails weitergeleitet werden.

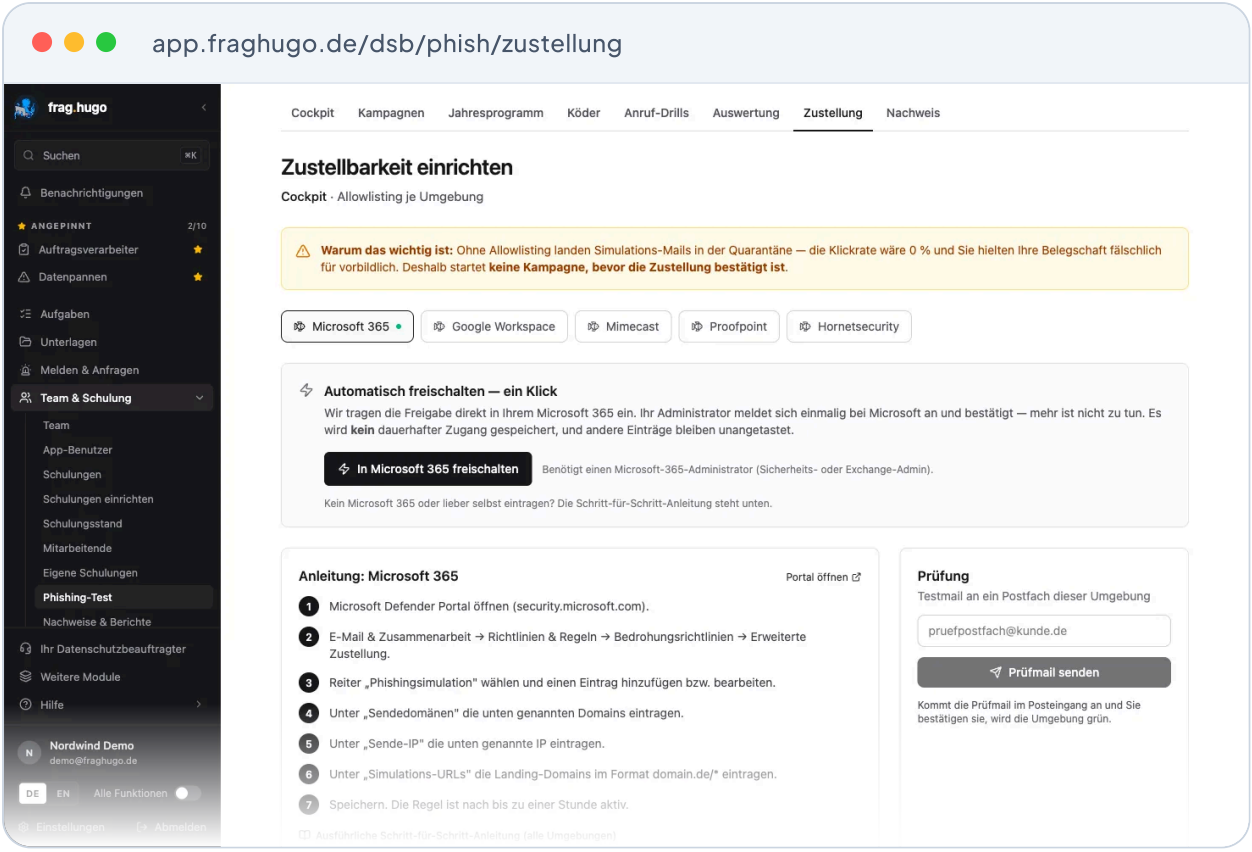
Anleitung Meldeknopf → (https://docs.fraghugo.de/hugo-phish/meldebutton/)

3

Erst an sich selbst schicken

Bevor eine Übung an alle geht, schicken Sie die gewählte Vorlage an Ihr eigenes Postfach und sehen sie genau so, wie Ihre Mitarbeitenden sie sehen werden.

Schnellstart in fünf Schritten → (https://docs.fraghugo.de/hugo-phish/schnellstart/)



Screenshot Der Zustell-Assistent führt Ihre IT Schritt für Schritt durch die Freigabe.

HÄUFIGE FRAGEN

Was Geschäftsleitung und IT als Erstes fragen

Sieht die Geschäftsleitung, wer geklickt hat?

Nein. Auswertungen gibt es erst ab fünf beteiligten Personen, und diese Untergrenze ist in der Datenbank durchgesetzt, nicht nur in der Oberfläche. Ein Modus mit Klarnamen gehört zur Premium-Stufe und setzt eine Betriebsvereinbarung voraus; jede Umstellung wird protokolliert. Mehr dazu im Betriebsrats-Paket.

Müssen wir dafür etwas installieren oder in der Firewall freigeben?

Auf den Rechnern der Mitarbeitenden wird nichts installiert. Die Übungs-Mails kommen auf dem normalen Mailweg an; Ihre IT trägt einmalig eine Freigabe im Mailfilter ein, damit sie nicht als echtes Phishing aussortiert werden. Der Meldeknopf wird zentral über Microsoft 365 verteilt. Die Schritte stehen in der Anleitung zur Zustellbarkeit (https://docs.fraghugo.de/hugo-phish/zustellbarkeit/).

Wir haben einen Exchange Server im eigenen Haus. Geht das trotzdem?

Ja. Die Freigabe läuft dort über eine Nachrichtenflussregel, die Anleitung steht in der Plattform. Der Meldeknopf lässt sich mit einem Exchange Server im eigenen Haus nicht laden; gemeldet wird dann über ein Melde-Postfach, die Meldungen fließen genauso in die Auswertung.

Was passiert, wenn jemand auf einer nachgestellten Anmeldeseite ein Kennwort eingibt?

Nachgestellte Anmeldeseiten gehören zur Premium-Stufe. Gemessen wird nur, dass etwas eingegeben wurde. Benutzername und Kennwort verlassen den Browser nicht und werden nirgends gespeichert. Danach folgt dieselbe Aufklärungsseite wie nach einem Klick.

Können wir eine Übungs-Mail ansehen, bevor sie an alle geht?

Ja. Beim Planen gibt es den Knopf „Erst an mich schicken“. Sie bekommen die gewählte Vorlage in Ihr eigenes Postfach und sehen damit auch gleich, ob die Zustellung funktioniert.

Was sagen wir der Belegschaft vorher?

Dass geübt wird, aber nicht wann. In der Plattform liegt dafür eine Mitarbeiter-Information als Vorlage bereit, dazu eine Muster-Betriebsvereinbarung und ein Papier zu den Rechtsgrundlagen. Die Vorlagen ersetzen keine Rechtsberatung im Einzelfall.