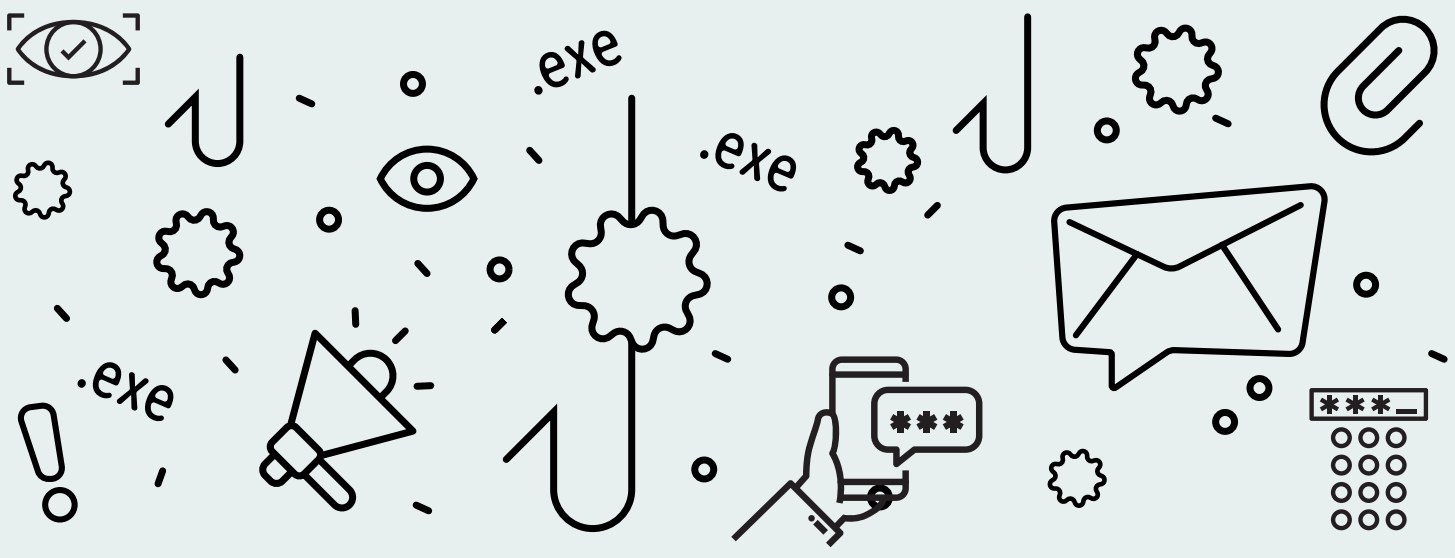


Betreff: Corona-Phishing: Schützen Sie sich vor kriminellen Mails

Sehr geehrte/r Frau/Mann Mustermann,

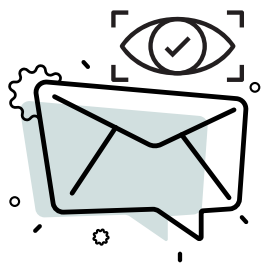
Atemschutzmasken, Desinfektionsmittel, sensationelle Forschungsergebnisse, Panik-News oder Spendenaufrufe: Täglich versenden Online-Kriminelle vermeintlich interessante Neuigkeiten rund um COVID-19 über E-Mail, Messenger oder soziale Netzwerke – und nutzen so die aktuelle Unsicherheit vieler Empfänger für betrügerische Aktivitäten aus.

Phishing Mails – was steckt dahinter?

Zusammengesetzt aus „Passwort“ und „Fishing“ bringt der Begriff es auf den Punkt: Es geht um das Fischen nach Passwörtern und sensiblen Daten. Die täuschend echt gestalteten Nachrichten erwecken den Eindruck eines vertrauenswürdigen Absenders und fordern in höchster Dringlichkeit auf, Links zu klicken und auf perfekt imitierte Websites vertrauliche Informationen wie Zugangsdaten oder Kreditkartennummern einzugeben.

Leider funktioniert diese kriminelle „Masche“ gerade in Notsituationen besonders gut. Daher möchten wir Sie zur digitalen Wachsamkeit aufrufen und Sie dabei mit einigen Tipps unterstützen.

Wie können Sie sich und Ihre Daten vor Phishern schützen?



Tipp 01

Prüfen Sie die Mail auf Echtheit

Wenn Sie von uns Mails erhalten, dann tragen diese stets die Absenderadresse *[support@unternehmen.com]*. Wir sprechen Sie immer persönlich und mit vollständigem Namen an.

Tipp 02

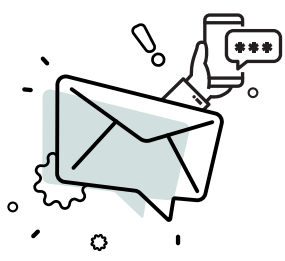
Geben Sie keine persönlichen Daten und Passwörter preis

Wir fordern Sie niemals in E-Mails auf, persönliche Daten wie Passwörter über einen Link zu ändern – also, klicken Sie nicht auf solche Links, ganz gleich wie dringend Sie dazu aufgefordert werden.

Tipp 03

Vorsicht bei Anhängen mit .exe, .scr oder .pdf.exe

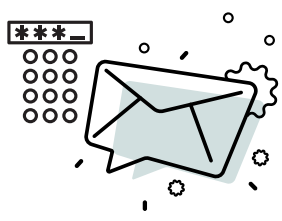
Solche Formatanhänge sollen Sie sofort skeptisch machen. Dahinter stehen oftmals Malware-Programme, die Schadsoftware direkt auf Ihr Gerät laden. Am besten solche Anhänge nicht öffnen – gleiches gilt für verdächtige Links.



Tipp 04

Setzen Sie auf die „doppelte“ Authentifizierung

Neben dem klassischen Kennwort schützen wir Sie mit dem sogenannten „zweiten Authentifizierungsfaktor“ als Barriere beim Einloggen. So wird meist ein Code per SMS oder in separater App übermittelt, den Sie dann zusätzlich eingeben müssen. Selbst wenn Ihr Account gehackt wurde, kann so oft und schnell Schlimmeres verhindert werden.



Tipp 05

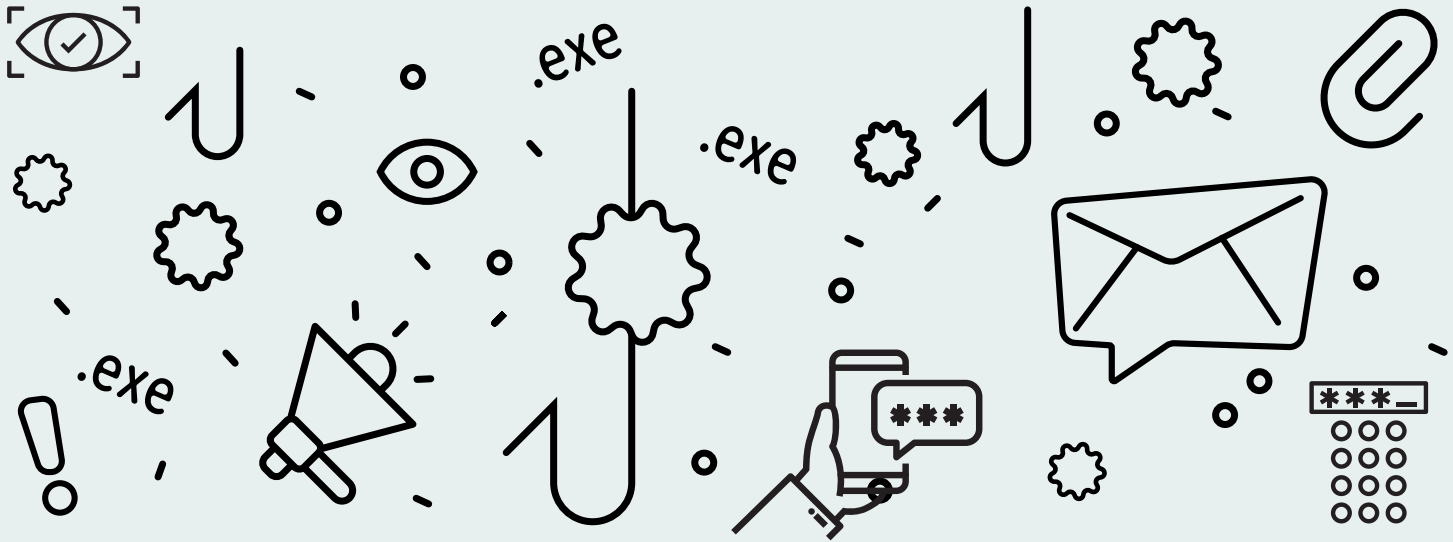
Achten Sie auf die Zahlarten

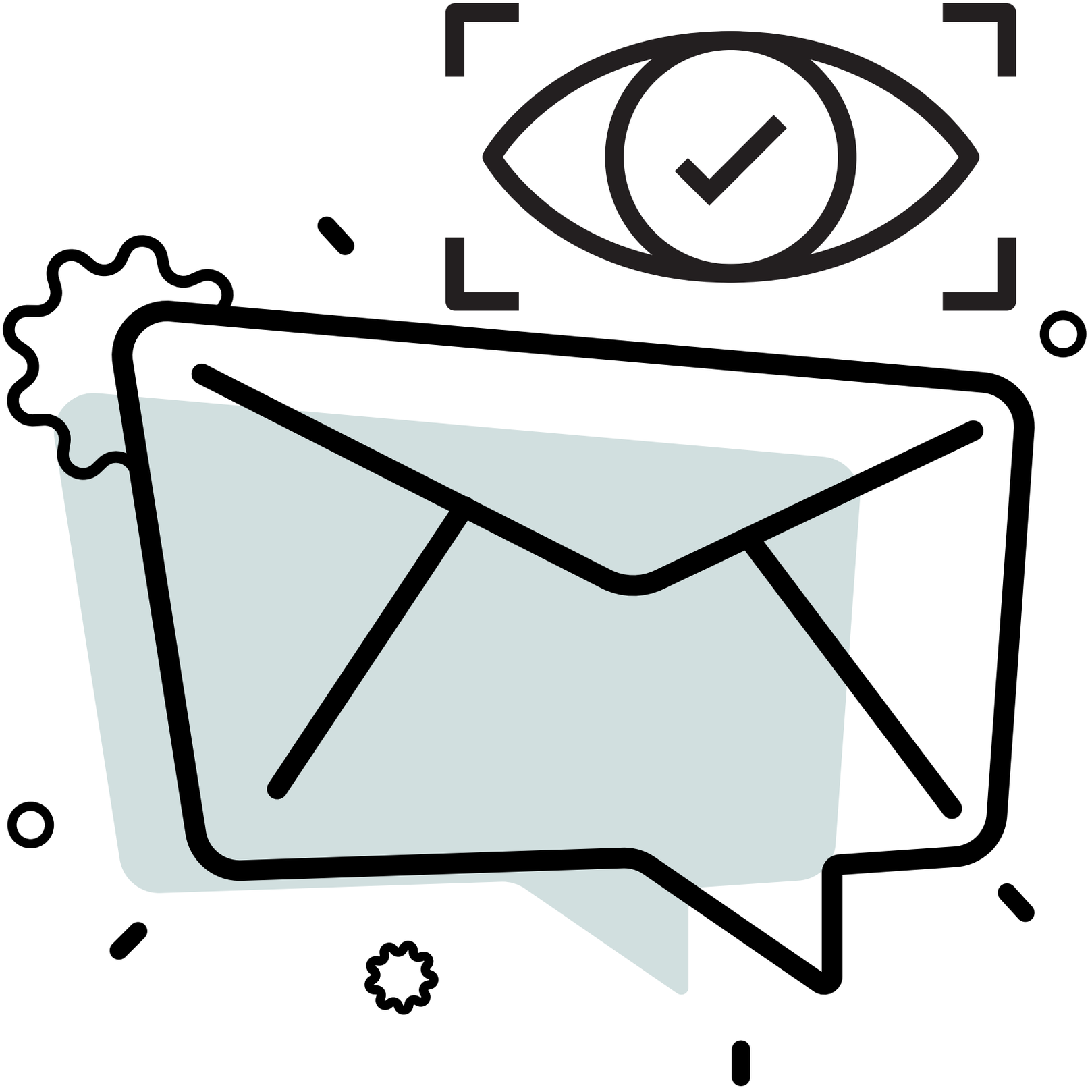
Wir verwenden ausschließlich folgende Zahlungsmöglichkeiten: PayPal, paydirekt, Kauf auf Rechnung und Kreditkarte. Weitere Zahlungsmethoden bieten wir nicht an. Seien Sie skeptisch im Falle anderer Zahlarten – dies weist auf einen Phishing-Versuch hin.

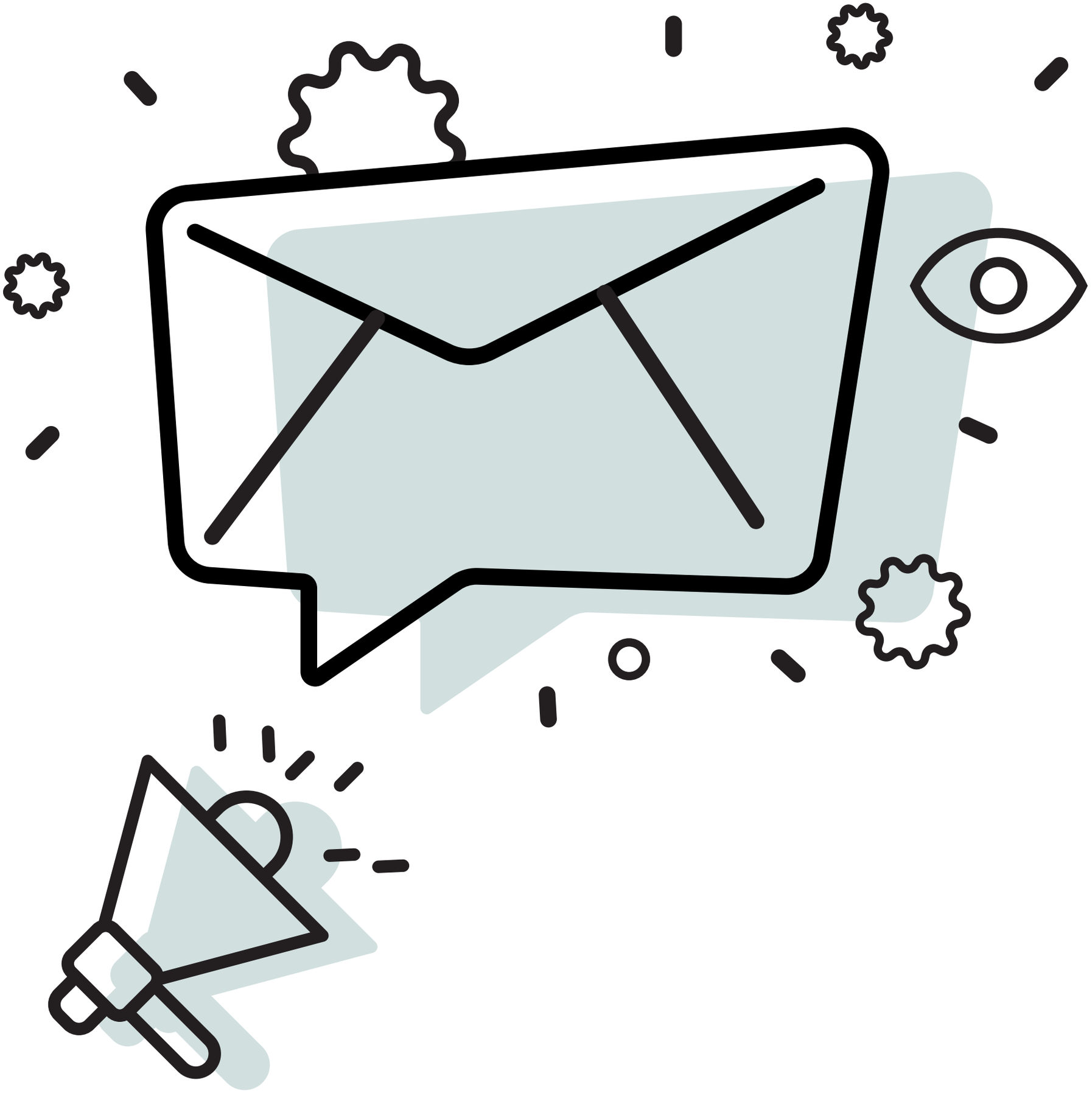
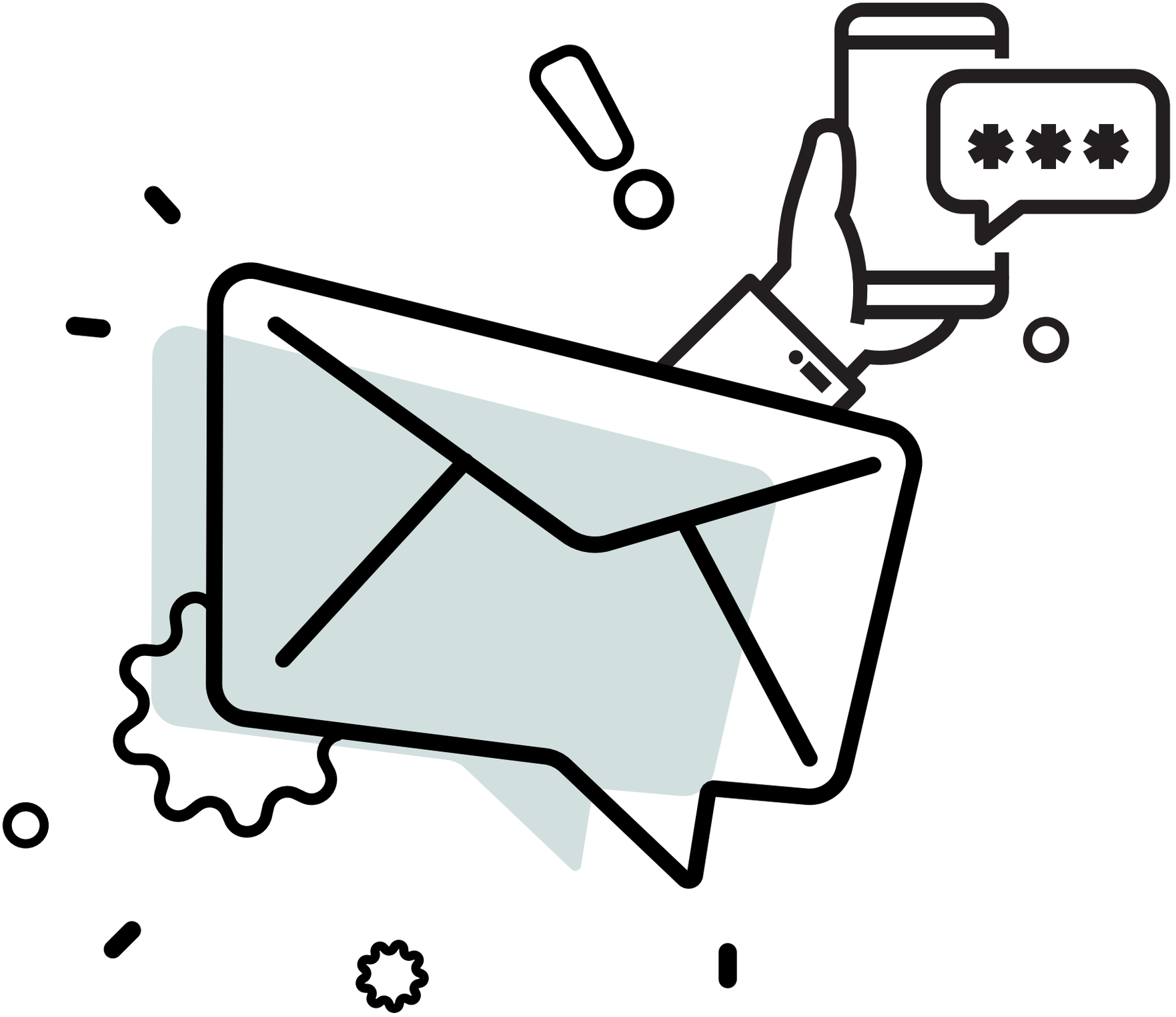
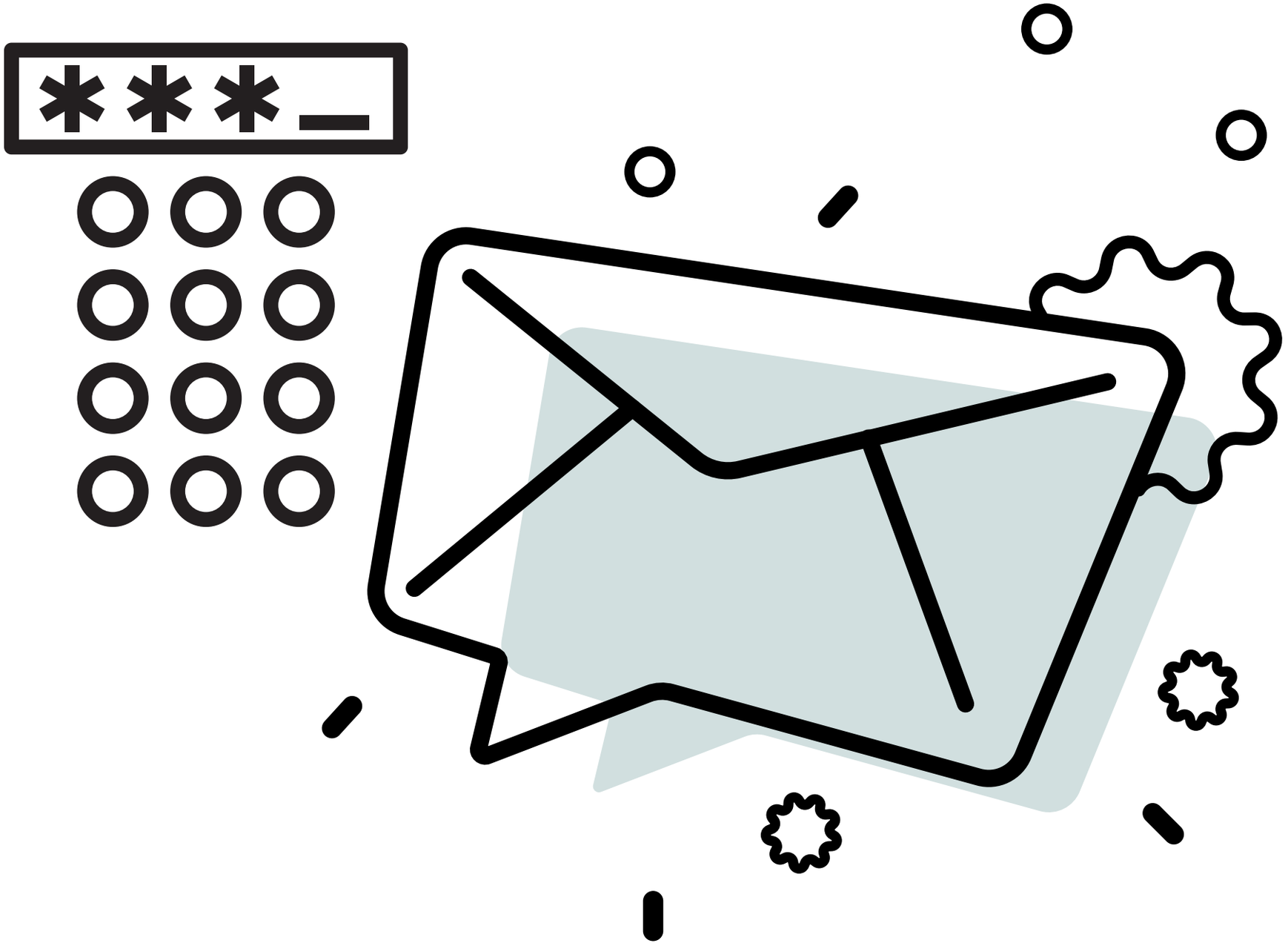
Wie vielversprechend eine Mail auch klingen mag, bleiben Sie kritisch und prüfen Sie die Inhalte lieber doppelt und dreifach. Im Zweifel, einfach löschen. In diesem Sinne: Bleiben Sie sicher und vor allem gesund.

Mit freundlichen Grüßen
(Absender)

Sie haben Fragen zum Thema Cyber-Kriminalität?
Unser Security-Team hilft Ihnen gerne weiter: *[support@unternehmen.com]*


.exe
.exe
.exe
***
***_





.exe