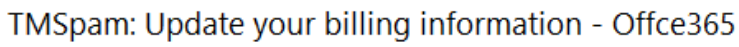
IT-Sicherheit im Unternehmen – Zusammenfassung für Kunden

1. E-Mail-Überprüfung

Phishing: Phishing ist eine Betrugsmethode, bei der Angreifer gefälschte E-Mails, SMS oder Webseiten nutzen, um Menschen dazu zu bringen, vertrauliche Daten wie Passwörter oder Bankinformationen preiszugeben. Die Nachrichten wirken oft täuschend echt und erzeugen Druck oder Dringlichkeit, damit Betroffene unüberlegt handeln. Ziel ist immer, Zugang zu Konten oder zu persönlichen Daten zu erhalten und finanziellen Schaden anzurichten.

Merkmale von Phishing Mails:

1. Technische Warnhinweise von Ihrem E-Mail-Programm: Viele Programme markieren verdächtige Inhalte – diese Hinweise sollte man ernst nehmen.
Beispiel: Der Virenscanner Trend Micro markiert eine Mail als Spam (TMSpam)

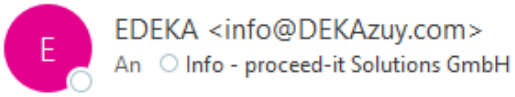


2. Unbekannter Absender: Kenne ich den Absender? Wenn die Mail echt sein könnte: auf weitere Merkmale prüfen.

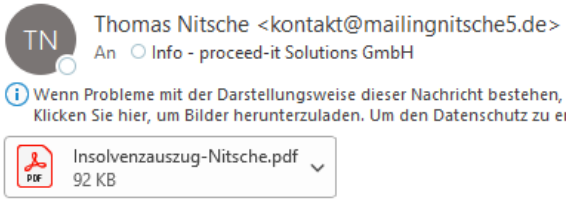
3. Ungewöhnlicher Absender: Die E-Mail-Adresse passt nicht zu dem angeblichen Unternehmen.
Beispiel: Unterschrieben wird mit Postbank, aber die E-Mail-Adresse ist support@performancezyanmalkar23.nl

4. Merkwürdige Mail vom „bekannten" Absender: Eine E-Mail kommt angeblich von einer firmeninternen E-Mail-Adresse, aber die Nachricht ist fragwürdig
Achtung! Eine E-Mail kann sogar so aussehen, dass sie vor der richtigen E-Mail-Adresse kommt. Kommt Ihnen der Inhalt merkwürdig vor, fragen Sie beim Absender nach.
Beispiel: Sie werden von der Finanzabteilung gefragt, ob eine Zahlung freigegeben werden soll.

5. Unterschied zwischen Anzeigename und echter Adresse: Der angezeigte Absendername kann gefälscht sein – entscheidend ist die tatsächliche Absenderadresse.
Beispiel: Oben in der Absenderzeile steht EDEKA, aber die Mail kommt von der E-Mail-Adresse info@DEKAzuy.com

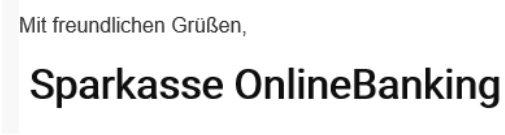


6. Unerwartete Anhänge oder Links: Dateien oder Links können Schadsoftware enthalten. Fragen Sie: Erwarte ich von dieser E-Mail-Adresse einen Anhang oder Link?
Beispiel:

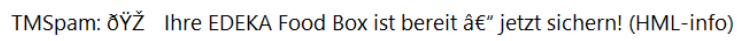


7. Persönliche Ansprache fehlt
Beispiele: Sie werden mit „Sehr geehrter Nutzer“, „Hallo“, „Dear Customer“ angesprochen

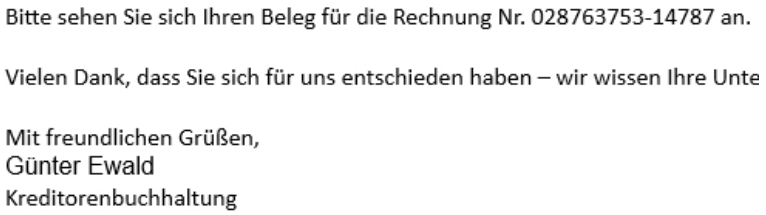
8. Unterschrift und/oder Signatur fehlt
Beispiel:



9. Fehlerhafte Sprache, komische Zeichen oder seltsame Formulierungen: Tippfehler, ungewöhnliche Satzstellungen oder merkwürdige Grammatik in der E-Mail.
Anmerkung: Bereits heute wird der Großteil von Phishing-Mails mit KI geschrieben, wodurch sie in Sprache immer besser werden.
Beispiel:



10. Unstimmige Formatierung: Der Text in der E-Mail, z. B. der Unterschrift ist anders formatiert als der restliche Teil des E-Mails
Beispiel: Unterschrift sieht anders aus



11. Falsches oder kopiertes Design: Logos und Layouts können täuschend echt aussehen, aber oft wirken sie leicht „anders“.
Beispiel: Stempel ist „gequetscht“ und hat merkwürdige Buchstaben

12. Links, die woanders hinführen: Halten Sie die Maus über einen Link in der E-Mail. Klicken Sie den Link **NICHT** an! Der angezeigte und der tatsächliche Link weichen voneinander ab.
Beispiel:

13. Unlogische Aufforderungen: Seriöse Firmen fragen niemals per E-Mail nach Passwörtern, Codes oder sensiblen Daten.

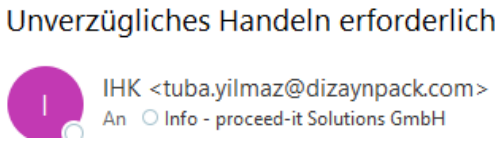
Beispiele: Sie werden aufgefordert, eine Rechnung zu bezahlen, ein Konto zu bestätigen, Anmeldedaten zu ändern, Ihren Namen zu überprüfen, eine Identitätsprüfung vorzunehmen oder Nachrichten freizugeben

14. Unpassende oder zu gute Angebote: Überzogene Gewinne, Prämien, Rabatte oder Versprechungen dienen oft als Köder.

Beispiel:

15. Dringlichkeit oder Druck: Formulierungen wie „sofort handeln“ oder „letzte Warnung“ sollen Sie zu schnellen Fehlern verleiten.

Beispiel:



16. Gefälschte Login-Seiten: Wenn die Adresse im Browser nicht exakt mit der echten Domain übereinstimmt, sollten Sie nichts eingeben.

Beispiel:

Echte Seite ist https://www.paypal.com (mit kleinem „L“ im Domain-Namen)

Gefälschte Variante: https://www.paypaI.com (großes „i“ statt kleiner „L“)

→ solche Unterschiede sind sehr schwer zu erkennen!

2. Weitere Sicherheitshinweise

Kennwort-Sicherheit

- Schreiben Sie Passwörter nicht Zetteln auf und speichern sie auch nicht in unverschlüsselten Dateien auf Ihrem Rechner.
- Erstellen Sie einzigartige und sichere Passwörter.
- Speichern Sie keine Passwörter in Ihrem Browser.
- Geben Sie keine Passwörter in Chats oder E-Mails weiter.
- Benutzen Sie ein Passwort-Tresor wie KeePass.
- Verwenden Sie Zwei-Faktor-Authentifizierung wie einen Authenticator

Computer mit Bedacht nutzen

- Seien Sie aufmerksam und achten Sie auf ungewöhnliche Aktivitäten auf Ihrem Rechner.
- Ignorieren Sie keine Fehlermeldungen und Warnfenster. Bedenken Sie aber: Warnfenster können auch gefälscht sein!
- Beim Verlassen des Arbeitsplatzes: sperren Sie Ihren Rechner mit der Tastenkombination Windows + L.
- Lassen Sie keine vertraulichen Daten offen liegen.

Nehmen Sie keine Anrufe von Microsoft, PayPal, etc. ernst

- Seriöse Firmen rufen niemals ungefragt an.
- Spätestens wenn jemand um Zugangsdaten oder um einen Zugriff zu Ihrem Rechner bittet, seien Sie misstrauisch und legen Sie auf. Informieren Sie uns bei einem solchen Vorfall.

Schützen Sie Ihre Daten vor Verlust

- Speichern Sie Ihre Daten auf dem Server statt Lokal.
- Benutzen Sie ein gutes Backup-System, um Ihre Daten regelmäßig zu sichern.
- Sofort Bescheid geben, wenn Daten unerwünscht gelöscht oder verschoben wurden. Je früher, desto besser.

Installieren Sie keine Programme selbst (wenn Sie sich nicht sehr gut auskennen)

- Prüfen Sie, ob die Anbieter seriös sind.

Keine fremden USB-Sticks anschließen

- Ausschließlich firmeneigene, geprüfte Speichermedien benutzen.
- Fremde USB-Sticks können Viren oder Schadsoftware enthalten.

Wenn etwas passiert…

- Ziehen Sie den LAN-Kabel/trennen Sie das Gerät vom Internet. Machen Sie Screenshots, notieren Sie was passiert ist. Melden Sie sich bei uns, damit wir den Vorfall zügig behandeln können.
- Bei Unsicherheit, Fragen oder komischen Computeraktionen wenden Sie sich an uns.
- Nichts vertuschen! Es gibt keine blöden Fragen. Je schneller wir Bescheid wissen und reagieren können, desto besser können wir Ihnen helfen.