

Schutz gegen Phishing-Mails

Was sind Phishing-Mails?

Betrüger verschicken zahlreiche E-Mails an gezielt ausgewählte Empfänger und geben sich als Ivoclar Vivadent aus. Sie fordern Nutzer auf, beispielsweise eine vermeintliche Rechnung herunterzuladen, Bankverbindungen zu ändern oder Nutzerdaten zu aktualisieren. Wer auf den Link klickt, startet direkt einen Download einer schadhafenden Software und installiert in Folge einen Virus oder ein anderes Schadprogramm. Auch geben sich die Betrüger seit neuestem als Ivoclar Vivadent Mitarbeiter aus und fordern die Nutzer auf gefälschte Rechnungen zu bezahlen.

Generell gilt: Phishing-Mails immer löschen und nicht auf den Link klicken!

Schutz gegen Phishing-Mails

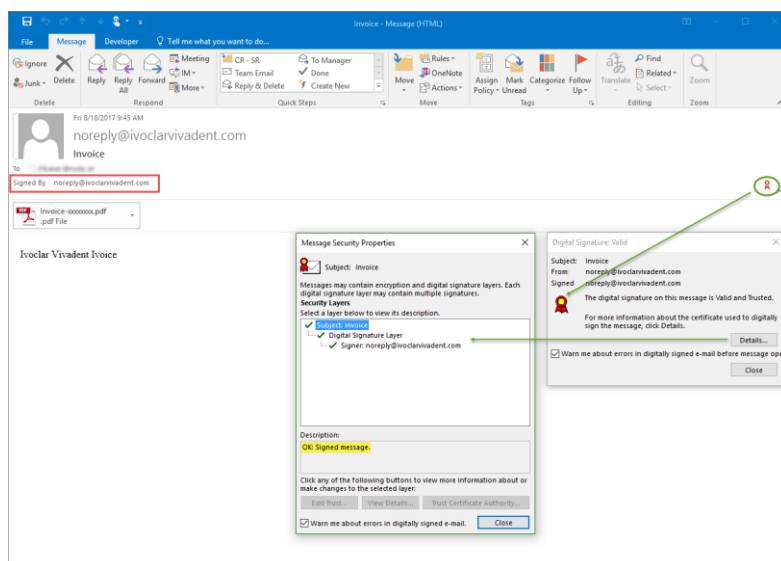
Ivoclar Vivadent kann den Versand von Phishing E-Mails nicht beeinflussen, um die Authentizität eines E-Mails zu gewährleisten versendet Ivoclar Vivadent jedes E-Mail mit einer digitalen Unterschrift, auch „digitale Signatur“ genannt.

Digital signierte E-Mails

Bei digital signierten Mails kann der Empfänger sicherstellen, dass alle Inhalte ohne Manipulation bei ihm angekommen sind, und der Sender tatsächlich der ist, der er vorgibt zu sein.

Erkennung eines digital Signiertes E-Mail.

Die digitale Signatur bei E-Mails erkennt man an einem grafischen Symbol oder einem Text im Bereich der Angabe des Absenders der E-Mail. Wie genau die Anzeige erfolgt, ist abhängig von E-Mail-Programm und Gerät und kann daher unterschiedlich sein. Beispielsweise blendet Microsoft Outlook unter dem Feld „An“ den Text „Signiert von: noreply@ivoclarvivadent.com“ ein und rechts am äußeren Rand der E-Mail wird ein Zeichen für eine Signatur angezeigt.



Kann die digitale Signatur gefälscht werden?

Ja - genauso, wie eine nicht-elektronische Unterschrift. Wird eine digitale Signatur gefälscht, kann das aber erkannt werden durch:

- Die E-Mail Anwendung zeigt eine Warnung an.
- Die Absender E-Mail-Adresse in der digitalen Signatur ist falsch. Beachte dabei bitte die E-Mail-Adresse, die in der Signatur aufscheint und nicht die Adresse, welche in deiner E-Mail angezeigt wird.

Das E-Mailprogramm unterstützt keine digitale Signatur oder unterstützt S/MIME nicht. Bedeutung des Anhangs „smime.p7s“?

Im Zuge des digitalen Signierens wird die Datei smime.p7s erstellt und der E-Mail als Anhang hinzugefügt. Kann die E-Mail-Anwendung nicht mit digitalen Signaturen umgehen, dann zeigt es nur einen Anhang mit dem Namen smime.p7s an oder das E-Mail kann nicht geöffnet werden. Das E-Mailprogramm kann daher die Signatur nicht überprüfen. Damit die digitale Signatur überprüft werden kann sollte immer ein aktueller E-Mail Client und ein aktuelles Betriebssystem benutzt werden. Die meisten Webmail Clients können digitale Signaturen nicht darstellen. Aus diesem Grund sollte immer ein am Computer installierter E-Mail Client verwendet werden.

IT Tipp:

Sehr alte Betriebssysteme (Windows XP, Windows Vista) oder E-Mail Clients (Outlook 2003, Windows Live Mail) können teilweise digital signierte E-Mail gar nicht darstellen. Abhängig vom eingesetzten E-Mail Client kommt eine Fehlermeldung beim Öffnen der signierten E-Mail. Ist dies zutreffend, sollte das Betriebssystem oder den E-Mail Client aktualisiert werden, da Microsoft keine Sicherheitsupdates zum Schutz des Computers mehr bereitstellt. Siehe auch: <https://support.office.com/de-de/article/Der-Support-f%C3%BCr-Office-2003-wurde-eingestellt-c5118100-b738-4163-b7c1-b9c4fe5b6b90>