Protection from email phishing

What is phishing?

Fraudsters send out deceptive emails purporting to be from Ivoclar Vivadent and targeting selected recipients. They request users to download a fake invoice, for example, or change bank credentials or update user data. These emails frequently contain a link, which, when clicked, will launch the download of an intrusive software that leads to the installation of a virus or other malware. Lately, some attackers have even started passing themselves off as Ivoclar Vivadent employees and requesting users to pay counterfeit invoices.

The general rule: Immediately delete phishing emails and do not click the link!

Protection against phishing attacks

Ivoclar Vivadent is unable to prevent the spread of phishing emails. In order to ensure the authenticity of emails sent by the company, a digital signature is added to all outgoing email messages at Ivoclar Vivadent.

Email messages with digital signature

When receiving an email message with a digital signature, recipients can be sure that the new contents that have arrived in their inbox have not been manipulated and the sender is actually the person he/she claims to be.

How to recognize a digitally signed email message

Digitally signed email messages contain a graphic symbol or additional text in the area of the Sender header. How exactly the digital signature is displayed depends on the email program and the hardware used and may thus vary. Microsoft Outlook, for example, inserts the text "Signed by: noreply@ivoclarvivadent.com" below the "To" box and displays a symbol representing the signature in the outer right hand margin.
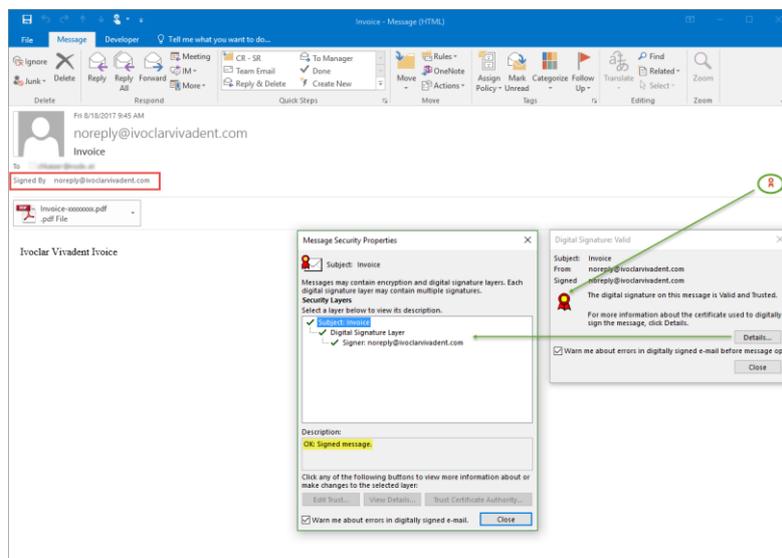
Can digital signatures be forged?

Yes, just like handwritten signatures. However, forged digital signatures can be recognized:

- The email application will show a warning.

- The Sender address in the digital signature will be incorrect (make sure to check the email address in the signature, not the one in your email!).

The email program does not support digital signatures or S/MIME.
What is a smime.p7s email attachment?

When an email message is digitally signed, a smime.p7s file is created and attached to the email. If the email application cannot handle digital signatures, it either only displays an attachment with the file name smime.p7s or the email cannot be opened. In this case, the email program cannot check the signature. To make sure that the digital signature is verified, always use an up-to-date email client or operating system. Moreover, an email client installed on a computer should always be used, as most webmail clients cannot display digital signatures.

Tip from the IT department:

Very old operating systems (Windows XP, Windows Vista) or email clients (Outlook 2003, Windows Life Mail) are often unable to display digitally signed emails. Depending on the email client installed, an error message will be displayed when the signed email is opened. In this case the operating system or email client should be updated as Microsoft no longer provides security updates to protect your computer. Also see: https://support.office.com/de-de/article/Der-Support-f%C3%BCr-Office-2003-wurde-eingestellt-c5118100-b738-4163-b7c1-b9c4fe5b6b90