HOW TO SPOT SCAM EMAILS

Email continues to be one of the easiest ways for hackers to gain access to your business. And all it takes is one incident to bring your operations to a halt. Here, we share some helpful tips on how to spot a scam email.

THE SENDER'S ADDRESS

The “From” line may include an official-looking address that mimics a genuine one.

TYPOS/POOR GRAMMAR

Emails sent by popular companies are almost always free of misspellings and grammatical errors.

FAKE LINKS

Check where a link is going before you click on it by hovering over the URL in an email and comparing it to the URL in the browser. If it looks suspicious, don’t click it.

GENERIC GREETINGS

Be wary of impersonal greetings like “Dear User.” Most legitimate emails will greet you by your username, email or name.

FALSE SENSE OF URGENCY

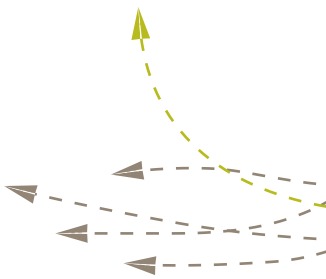
Many scam emails will tell you that your account will be in jeopardy if something critical is not updated right away.

ATTACHMENTS

Be suspicious of company emails that include an attachment. Never open an attachment unless you are 100% sure it’s legitimate, because they can contain spyware or viruses.

CLICKING ON LINKS

Never click on a link in an email that requests personal information. Any time you receive an email about your account, open a new browser, type in the URL and login to your account directly.



For information or advice for securing your inbox, get in touch with us at contact@ka2.io