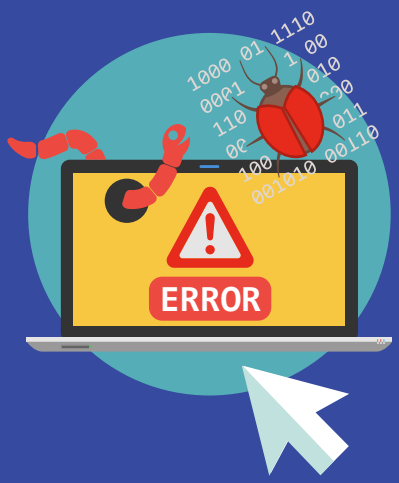
SPOOFED BANK WEBSITES

Bank phishing emails usually include links that will take you to a spoofed bank website, where you are requested to divulge your financial and personal information.

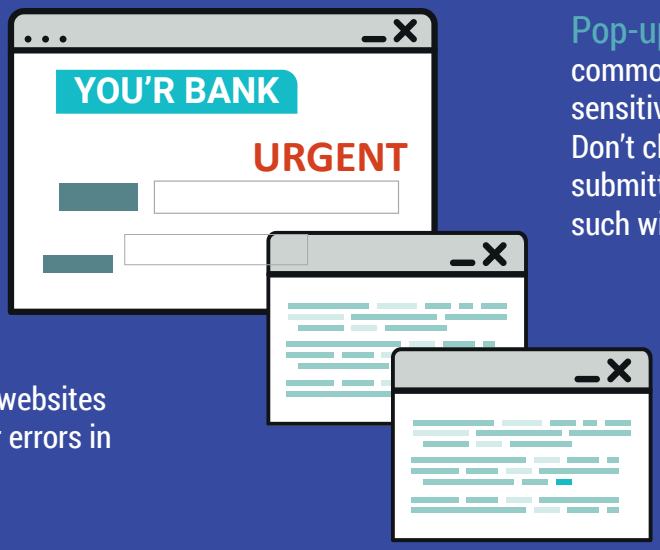


WHAT ARE THE SIGNS?

Spoofed bank websites look nearly identical to their legitimate counterparts. Such websites will often feature a pop-up window asking you to enter your bank credentials. Real banks don't use such windows.

These websites usually display:

Urgency: you will not find such messages on legitimate websites.



Pop-up windows: they are commonly used to gather sensitive information from you. Don't click on them and avoid submitting personal data on such windows.

Poor design: be cautious with websites that have flaws in their design or errors in spelling and grammar.

WHAT CAN YOU DO?

Never click on links included in emails leading to your bank's website.

Always type the link manually or use an existing link from your 'favourites' list.

Use a browser that allows you to **block pop-up windows**.

If something important really needs your attention, you will be alerted about it by your bank **when you access your on-line account**.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | Politie Police | febelfin | CYBER SECURITY COALITION | #CyberScams