SOCONNECT™
inspired communications

☎ 0333 240 1824 ✉ sales@soconnect.co.uk 🌐 www.soconnect.co.uk

Learn How to Detect a Phishing Email

1 Suspicious Sender

Cybercriminals use various spoofing techniques to trick users into believing an email is legitimate. Check the domain closely for close 'cousin' domains. Be cautious when reading email on your mobile device, as only the display name may be visible even if the email is bogus.

2 Subject Line & Tone

Enticing, urgent, or threatening language is commonly used to encourage the recipient to take immediate action. Evoking a sense of curiosity, greed, or fear is a common tactic among phishing schemes.

3 Greeting

Phishers often send out mass emails to gather information, so they use generic greetings. But, sophisticated phishers personalise their emails with information such as names, email addresses, and even breached passwords.

4 Errors

Read the email carefully. Grammatical errors are an obvious red flag, but sophisticated hackers do not make glaring errors. Instead, there may be more subtle mistakes, such as minor spacing issues or use of symbols instead of words. In some cases, there will be no errors.

5 Links

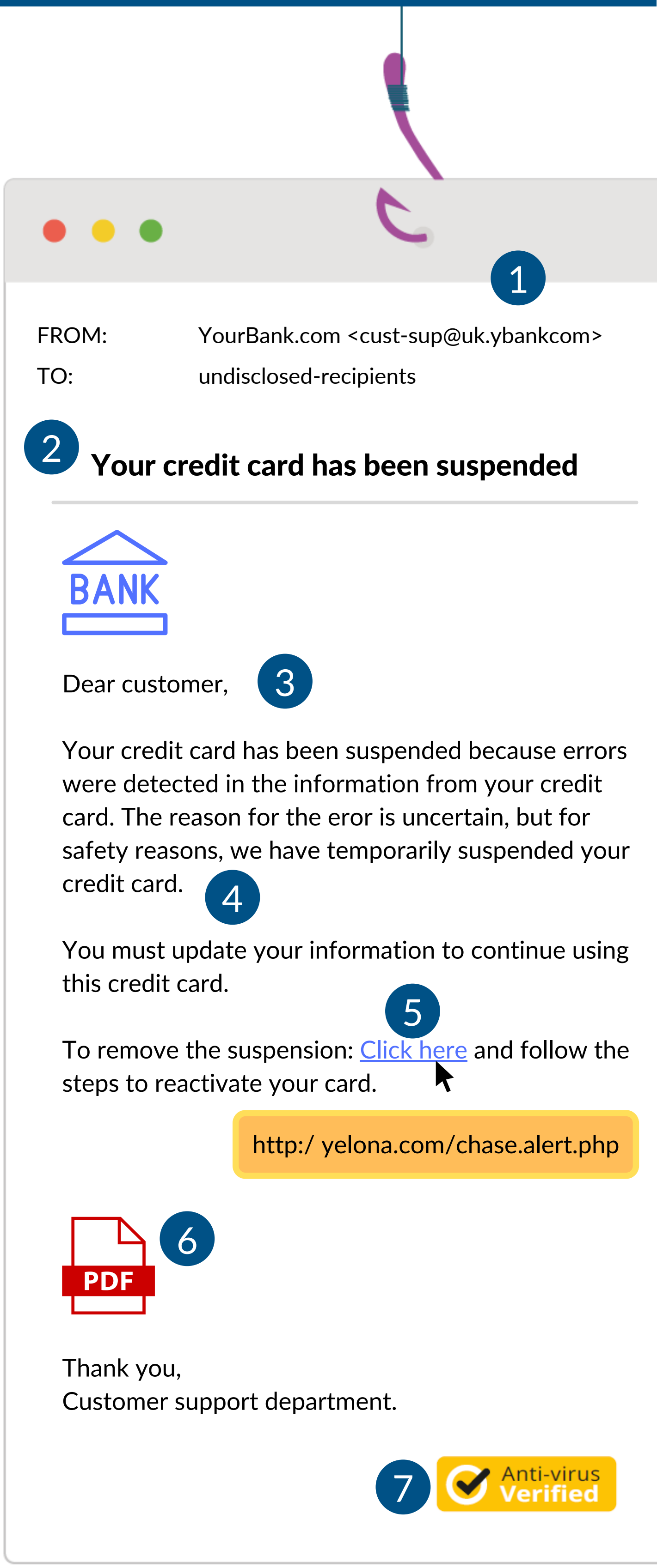
Before clicking, hover over the link to see the URL of where the link actually leads, and beware of link shorteners, such as Bitly or Ti-nyURL. Keep in mind that phishing emails can include clean URLs in addition to the phishing URL to trick users and email filters.

6 Attachments

Be wary of emails that include attachments. Phishing emails may include a link in an attachment, rather than the body of the email, to avoid detection by an email filter.

7 Images

Cybercriminals can easily replicate brand logos, images, and badges in emails and webpages that are indistinguishable from the real thing. Consider all the above factors as you decide whether to click.



FROM: YourBank.com <cust-sup@uk.ybankcom>
TO: undisclosed-recipients

Your credit card has been suspended

Dear customer,

Your credit card has been suspended because errors were detected in the information from your credit card. The reason for the eror is uncertain, but for safety reasons, we have temporarily suspended your credit card.

You must update your information to continue using this credit card.

To remove the suspension: Click here and follow the steps to reactivate your card.

http:/ yelona.com/chase.alert.php

Thank you,
Customer support department.

When in doubt, check it out

IsItPhishing.AI is a free service powered by our security partner Vade that performs real-time analysis of the URL and web page to determine if it's phishing.

Cyber Security Solutions

The latest government research suggests that Four in Ten (39%) of UK businesses identified at least one cyber attack or a breach in the last 12 months.

We help businesses across the UK **prevent around 99.3% of the most common cyber attacks.** Through a government-backed scheme, **Cyber Essentials**, we implement fundamental security controls which can minimise risk against the most common security threats. To find out more about gaining **Cyber Essentials** certification please get in touch with our team to arrange a free consultation.

WatchGuard	**Next-Gen Firewalls** WatchGuard's firewalls integrate next-generation firewall and deep learning technologies to help you identify, block, and respond to known and unknown threats such as malware, ransomware, cryptojacking, and more.
KEEPER	**Password Manager** Keeper is the top-rated personal and business password manager for protection from password-related data breaches and cyber threats.
Microsoft	**Microsoft 365 Secure** Microsoft 365 Secure is an exclusive productivity solution protected by Vade, backed up by Acronis Cloud. Keeping your data safe and secure. Microsoft 365 Secure protects your business with intelligent security and provides backup with instant recovery
Bitdefender	**Anti-Virus and Anti-Malware** Encompassing more than just anti-virus, the cybersecurity product brings a host of features that all aim to protect your device. Between anti-malware, anti-phishing and dual-layered firewalls, Bitdefender ensures your device is secure by detecting, anticipating and blocking all known or unknown attacks from its centralised cloud console.
CyberSmart	**Compliance Monitoring** Guarantee ongoing compliance with Cyber Essentials using our CyberSmart endpoints on all your employee's devices. CyberSmart fast-tracks the discovery and remediation of issues, protecting your firm from 99.3% of cyber attacks.