censornet.

BEC CHECKLIST

Business Email Compromise (BEC) is when an attacker pretends to be someone they aren't on email, typically senior management, to achieve their own ends. BEC costs organisations globally a staggering amount of money, but there are some simple steps you can take to put a stop to it.

TEN TOP TIPS

TO STOP BUSINESS EMAIL COMPROMISE FROM IMPACTING YOUR BUSINESS

1. Watch out for plain text emails appearing to come from the CEO / CFO or other senior management
2. Check the 'Reply to' address carefully – look for the use of nearby or cousin domains
3. CEO Fraud emails will be thoroughly researched and often target specifc members of the finance team who may need additional security or education
4. Implement a process for handling email requests to pay suppliers and make urgent bank transfers which involves contacting the originator directly to con rm any request
5. If a request or invoice can't be matched to a purchase order it should be investigated
6. Consider manual approval(s) for payments above a certain threshold
7. Repeatedly train all staff, not just the finance team, using examples of the latest phishing scams
8. Consider purchasing nearby domains (e.g. censornet.co, cens0rnet.com) to prevent their use in attacks
9. Protect user accounts such as Outlook Web Access with adaptive multi-factor authentication
10. Use a modern multi-layered email security solution that includes features to identify and quarantine/drop fraudulent emails, integrated domain name checking and executive tracking that identities real names in multiple address fields.

About censornet.

Headquartered in an innovation hub in Basingstoke, UK, Censornet gives mid-market organisations the confidence and control of enterprise-grade cyber protection. Its AI powered cloud security platform integrates attack intel across email, web, and cloud to ensure cyber defences react at lightning speed.

www.censornet.com