20 Tips to Deter Deepfake Phishing

Artificial intelligence (AI) allows scammers deploy sophisticated voice and email phishing attacks. Use these 20 tips to mitigate them.

1. Verify calls by hanging up and calling back the official number of the company or person.
2. Never share personal or financial information over the phone unless you initiated the call.
3. Be wary if the caller creates a sense of urgency or pressure to act quickly.
4. Listen for unnatural speech patterns or robotic-sounding phone voices.
5. Always double-check unusual requests for money transfers, especially from executives or coworkers.
6. Use multi-factor authentication for important accounts to add extra security.
7. Regularly update your passwords and avoid using the same password across multiple platforms.
8. Be suspicious of unexpected emails with urgent requests, especially those asking for money or sensitive information.
9. Examine email sender addresses for slight misspellings or unfamiliar domains.
10. Avoid clicking on links or downloading attachments from unknown or unexpected emails.
11. Verify any unexpected email requests for financial or sensitive information by contacting the sender through another means.
12. Set up email filters to block known phishing domains and addresses.
13. Use anti-phishing software and enable advanced email security features.
14. Check for inconsistent or awkward phrasing, poor grammar, or unusual greetings in emails.
15. Avoid sharing personal details on social media that scammers could use to impersonate you.
16. Regularly educate yourself on the latest phishing tactics and scams.
17. Implement strong security policies in your organization to minimize phishing risks for all employees.
18. Monitor your accounts for unusual or unauthorized activity.
19. Always report phishing attempts to your email provider or IT department.
20. Stay cautious when receiving communication outside normal business hours or on non-standard channels.

Barracuda®
Your journey, secured.