AI Text Phishing

Staying vigilant against emerging threats like AI text phishing is more important now than ever. Here's what you need to know.

What to watch for:

Check the Sender
Verify the sender's number. If it seems suspicious, be cautious.

Spelling and Grammar
Look for errors, which AI-generated messages can generate.

Urgent Requests
Be skeptical of urgent requests—scammers use pressure tactics.

Unsolicited Requests
Legitimate organizations won't ask for sensitive info via text.

Suspicious Links
Avoid clicking links. Instead, visit the official website directly.

If you receive one:

Don't Respond
Avoid replying or engaging with the sender.

Block the Sender
Block the number to prevent further communication.

Avoid Clicking Links
Never click on links or download attachments.

Report the Message
Report it as junk to your mobile carrier.

Stay Protected
Ensure your device has up-to-date mobile security.

Are you working today? I'm on the road and need login info. I'm usually not this forgetful! Thanks for helping out in a crisis!

They're saying this was a dismal quarter but I know an apples to apples comparison would prove it wasn't. Can you send me the shared link to last quarter's sales so I can set things right with management?

Not everyone will get a bonus this year. It's not fair, because you work so hard and I don't get why they can't see how you contribute!

I'm laughing because once again I'm locked out of the office on a weekend. Must have changed the entry PIN. Please send asap!

While traditional text fraud tends toward urgency and human actions, like clicking a link, AI text fraud uses machine learning to create emotionally manipulative texts that encourage further engagement.

Barracuda