

Protect Your Data Against Phone Fraud

While you are probably aware of the dangers of email fraud, the information you give over the phone is also vulnerable.



Phone fraud is becoming a **bigger threat than ever before.**



Criminals are now using Artificial Intelligence to impersonate voices, meaning the person on the phone **may not be who you think.**

In fact, the CEO of a global company was recently tricked out of \$243,000 by AI-generated “deepfake” voice technology.

- This tactic has cost companies an average of **\$2 billion over the past two years**
- Attackers often use email-based scams, like phishing and baiting, to start the process
- Fraudsters often impersonate a company’s **senior staff members**, giving them more power via social engineering and established trust



These “deepfakes” have the potential to harm your company, and consumers, by creating another way to make your data vulnerable.

Protect yourself, your clients, and your company by taking special care to **require additional verification** before providing:

- Sensitive, personal, or private data
- Payment or funding details
- Any information that is **not** readily available to the public