YOUR LOGO

Powered by PHIN

Your Guide to Spotting Scams in 2027

Cybercrime Doesn't Just Happen to Other People.

Cybercriminals target businesses of all sizes, and you don't need to be a CEO or work in IT to become a target. One convincing phishing email, stolen password, or fraudulent payment request can lead to financial losses, exposed information, and major disruptions. And now, with artificial intelligence (AI), scams are becoming harder to recognize.

$4.99M

Average global cost of a data breach in 2026.

247 Days

Average time to identify and contain a data breach.

$6M

Average cost of an AI-enabled malicious breach.

Source: IBM, Cost of a Data Breach Report 2026

Think you could spot a deepfake?

Only 0.1% Could.

In a 2025 study of 2,000 people, just 0.1% correctly identified every real and AI-generated image and video shown to them. Even when participants were warned to look for deepfakes, they struggled to distinguish real content from AI-generated fakes.

Source: iProov, 2025 Deepfake Detection Study.

With the evolution of AI, you can no longer rely on bad grammar, strange formatting, or even a familiar voice to identify a scam.

Scams aren't what they used to be...

(Print the third page of this guide for handy reminders.)

Scams Have Gotten Smarter. Have Your Security Habits?

AI has made it easier for cybercriminals to create convincing scams that look, sound, and feel legitimate. Here's what's changed:

Traditional Social Engineering	Modern Social Engineering
Poorly written phishing emails	Polished, professional, localized messages
Generic mass phishing campaigns	Personalized attacks using publicly available information
Static phishing emails	Interactive, AI-powered conversations
Caller ID spoofing	AI-generated voice impersonation
Fake profiles and stolen photos	Realistic AI-generated images and videos
Manual research and impersonation	Automated research and content generation

You don't need to be a cybersecurity expert to help protect your organization. Small actions can make a big difference:

Protect your accounts. Use strong, unique passwords and enable multi-factor authentication (MFA).

Question unusual requests, especially when they involve money, passwords, or sensitive information.

Verify before you act. Contact the person or company through a trusted channel you find independently.

Report suspicious activity. If something seems off, tell your IT or security team.

How to Spot Scams in 2027

While AI has given scammers the ability to target people on a larger scale and in more convincing ways, the psychological tactics they rely on haven't changed.

URGENCY

A false sense of urgency discourages you from thinking critically. "Your account will be suspended unless you verify your information immediately."

EMOTIONAL MANIPULATION

Scammers exploit fear, sympathy, excitement, and personal relationships to influence behavior. "I've been in an accident and need help. Please send money as soon as you can."

PRESSURE

Scammers may discourage you from asking questions, following procedures, or involving others. "This is confidential. Please handle it directly and don't involve anyone else."

THREATS

Attackers may use fear of consequences to manipulate decisions. "Failure to complete this could result in legal action being taken."

FINANCIAL REQUESTS

Watch for unexpected requests involving money, payment changes, or financial information. "We've changed banks. Please update our payment information before processing the next invoice."

Before responding to an email, text message, or phone call, **ask yourself:**

- **Was I expecting this message?**
- **Is the sender who they claim to be?**
  Check the actual email address or phone number, not just the display name.
- **Does the request make sense?**
  Be cautious of unusual requests involving money, passwords, or sensitive information.
- **Am I being pressured to act quickly?**
- **Can I verify this another way?**
  Use a known phone number, official website, or trusted communication channel.

AI allows scammers to impersonate people you know in audio, images, and videos. Anytime you experience an odd, unusual, or highly impactful request, **verify it via another communication channel that you trust.**