What's New

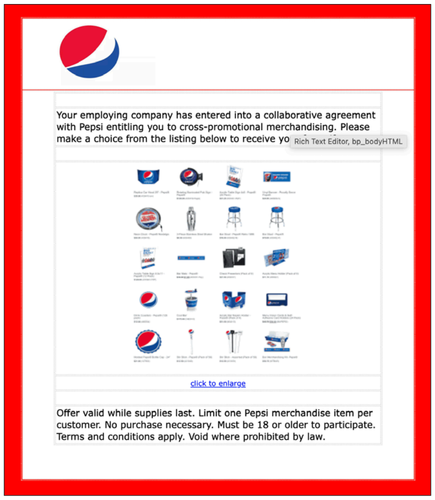
Here's a fresh look at the latest training content.

October 2024

Real World Threat Emails

These emails are based on emails flagged by Barracuda security and other real-world samples. Search for them by name in the SAT tool.

Pepsi Collaboration

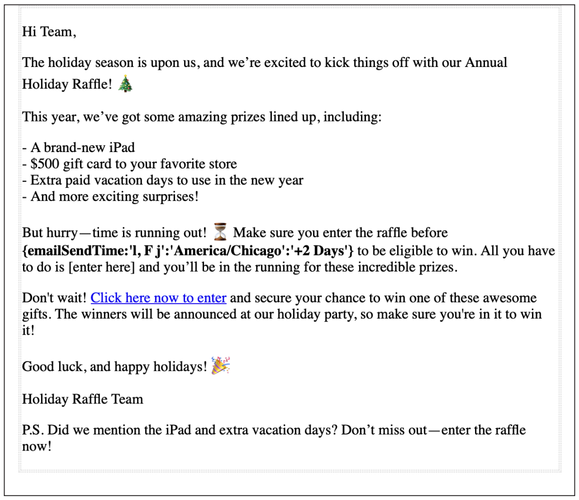


Your employing company has entered into a collaborative agreement with Pepsi entitling you to cross-promotional merchandising. Please make a choice from the listing below to receive yo

click to enlarge

Offer valid while supplies last. Limit one Pepsi merchandise item per customer. No purchase necessary. Must be 18 or older to participate. Terms and conditions apply. Void where prohibited by law.

Holiday Raffle



Hi Team,

The holiday season is upon us, and we're excited to kick things off with our Annual Holiday Raffle! 🎄

This year, we've got some amazing prizes lined up, including:

- A brand-new iPad
- $500 gift card to your favorite store
- Extra paid vacation days to use in the new year
- And more exciting surprises!

But hurry—time is running out! ⏳ Make sure you enter the raffle before **{emailSendTime:'l, F j':'America/Chicago':'+2 Days'}** to be eligible to win. All you have to do is [enter here] and you'll be in the running for these incredible prizes.

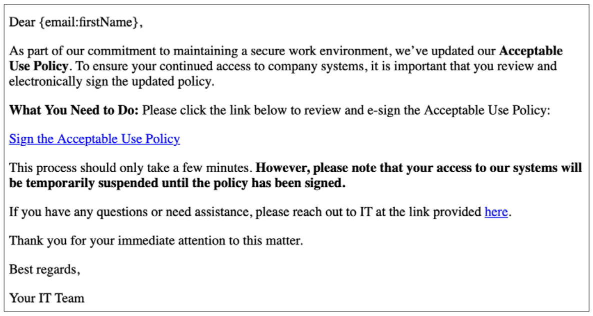
Don't wait! Click here now to enter and secure your chance to win one of these awesome gifts. The winners will be announced at our holiday party, so make sure you're in it to win it!

Good luck, and happy holidays! 🎉

Holiday Raffle Team

P.S. Did we mention the iPad and extra vacation days? Don't miss out—enter the raffle now!

Sign Updated Acceptable Use Policy



Dear {email:firstName},

As part of our commitment to maintaining a secure work environment, we've updated our **Acceptable Use Policy**. To ensure your continued access to company systems, it is important that you review and electronically sign the updated policy.

What You Need to Do: Please click the link below to review and e-sign the Acceptable Use Policy:

Sign the Acceptable Use Policy

This process should only take a few minutes. **However, please note that your access to our systems will be temporarily suspended until the policy has been signed.**

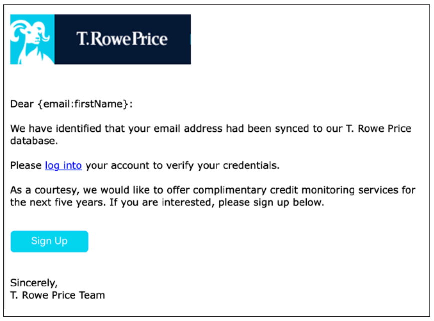
If you have any questions or need assistance, please reach out to IT at the link provided here.

Thank you for your immediate attention to this matter.

Best regards,

Your IT Team

T Rowe Credit Monitoring



Dear {email:firstName}:

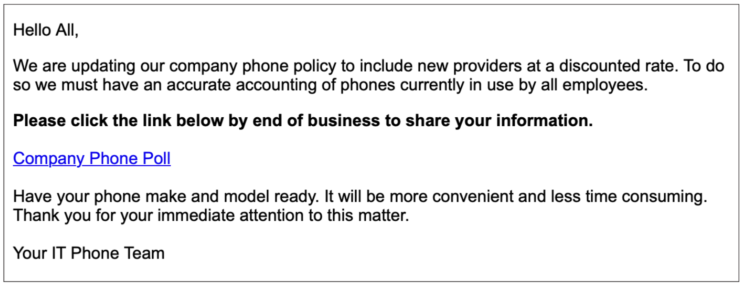
We have identified that your email address had been synced to our T. Rowe Price database.

Please log into your account to verify your credentials.

As a courtesy, we would like to offer complimentary credit monitoring services for the next five years. If you are interested, please sign up below.

Sincerely,
T. Rowe Price Team

Subsidized Phone



Hello All,

We are updating our company phone policy to include new providers at a discounted rate. To do so we must have an accurate accounting of phones currently in use by all employees.

Please click the link below by end of business to share your information.

Company Phone Poll

Have your phone make and model ready. It will be more convenient and less time consuming. Thank you for your immediate attention to this matter.

Your IT Phone Team

More on next page.

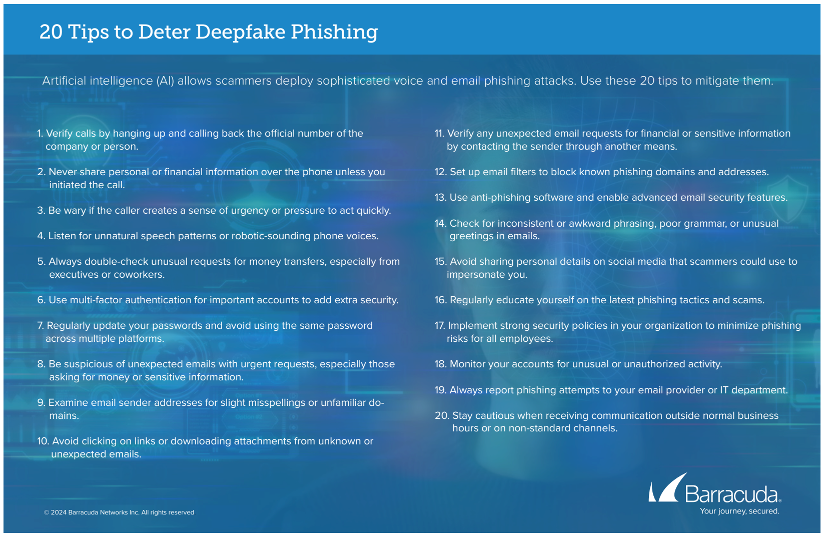
Barracuda

October 2024

Deepfake Phishing A103A-27

A new animated training module that provides insights into the motives and methods behind deepfake voice and email phishing scams along with tips to help recognize and mitigate them.

Deepfake Phishing Infographic



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.