

USEFUL WEB SITES

PHISHING

Recognizing and responding to Internet scams

U.S. Federal Trade Commission

Details on identity theft, with links to publications on phishing and other scams:

consumer.gov/idtheft/

U.S. Justice Department

An overview of identity theft and how the U.S. Department of Justice is taking action:

usdoj.gov/criminal/fraud/idtheft.html



If you have questions, contact the
T. Rowe Price Enterprise Help Desk
at 410-345-4357

WHAT IS “PHISHING?”

Phishing (pronounced “fishing”) is an Internet-based scam that extracts personal information from its victims through fraudulent e-mail, pop-up messages, or Web sites asking for users’ personal information. The scammers are attempting to obtain victims’ data, assets, identity, or all three.

Internet users may unknowingly surrender their logons, credit card numbers, passwords, banking details, or Social Security numbers to these legitimate-looking sources.

The perpetrators of phishing scams are careful to make their messages appear professional. They will often ask the Internet user to “update” or “confirm” sensitive data.

Some messages may link users to authentic-looking but phony Web sites. Or, a normal-looking e-mail might download spyware onto your personal computer, record your data, and send it back to the scammers.

T. Rowe Price urges all associates to be on guard for such scams. The information in this flyer will help us better protect our customers and ourselves.

HOW T. ROWE PRICE RESPONDS

Any time a customer asks you about an odd or suspicious e-mail that he or she received with T. Rowe Price’s name attached—especially one asking for sensitive information—you should be on alert, and quickly do the following:

1. Ask the customer to forward you the e-mail, or at least provide the contents or URL.
2. Contact your supervisor and the Help Desk immediately with any evidence of a suspicious e-mail or Web site.
3. Remind customers not to provide information or click on any links within suspicious e-mails.

Although the Firm must be cautious about giving our customers specific advice, we may recommend that they contact law enforcement. We may also refer the customer to the Federal Trade Commission’s Web site listed in this guide.

Computer professionals may be helpful in counseling the customer on malware issues.

E-MAIL ETIQUETTE

When communicating with customers by e-mail:

- Be sure to include the customer’s name in the salutation.
- Use correct business language in accordance with our brand standard.
- Do not include any of the customer’s own confidential information such as social security number or account number.
- Make sure your message includes proper contact information.
- Never ask the customer to convey or confirm sensitive personal information through an e-mail.

AVOID GETTING “REELED IN”

Anyone who uses the Internet or e-mail should be aware of these common sense precautions:

1. If you get an e-mail asking for personal or financial information, do not reply or click on any links contained in the e-mail.
2. Contact the business:
 - a. Open a new browser page and type the company’s URL in the address line or,
 - b. Call their official customer service phone number available on account statements or through the 800 number directory.
3. Keep your home computer’s anti-virus software up to date by downloading the most recent updates from the software company’s Web site. (T. Rowe Price updates your company computer’s anti-virus software for you on a regular basis.)
4. Monitor your banking and credit card statements carefully for unauthorized transactions.



USEFUL WEB SITES

U.K Home Office Identity Fraud Steering Committee

A collaboration between UK financial bodies, government and the police to combat the threat of identity theft. Contains details and advice on avoiding identity theft and what to do if you are a victim.

identity-theft.org.uk/

U.K. Banking Industry Site on Safe Online Banking

Details and advice on how to avoid becoming a victim of an internet scam with links to publications on phishing and other scams:

banksafeonline.org.uk/

National Hi-Tech Crime Unit

Information on high tech crimes targeting businesses and the general public (The NHTCU is part of the UK National Crime Squad):

nhtcu.org.uk/

**If you have questions, contact the
T. Rowe Price Enterprise Help Desk
at 410-345-4357**

PHISHING

Recognizing and responding to Internet scams



WHAT IS “PHISHING?”

Phishing (pronounced “fishing”) is an Internet-based scam that extracts personal information from its victims through fraudulent e-mail, pop-up messages, or Web sites asking for users’ personal information. The scammers are attempting to obtain victims’ data, assets, identity, or all three.

Internet users may unknowingly surrender their logons, credit card numbers, passwords, banking details, or Social Security numbers to these legitimate-looking sources.

The perpetrators of phishing scams are careful to make their messages appear professional. They will often ask the Internet user to “update” or “confirm” sensitive data.

Some messages may link users to authentic-looking but phony Web sites. Or, a normal-looking e-mail might download spyware onto your personal computer, record your data, and send it back to the scammers.

T. Rowe Price urges all associates to be on guard for such scams. The information in this flyer will help us better protect our customers and ourselves.

HOW T. ROWE PRICE RESPONDS

Any time a customer asks you about an odd or suspicious e-mail that he or she received with T. Rowe Price’s name attached—especially one asking for sensitive information—you should be on alert, and quickly do the following:

1. Ask the customer to forward you the e-mail, or at least provide the contents or URL.
2. Contact your supervisor and the Help Desk immediately with any evidence of a suspicious e-mail or Web site.
3. Remind customers not to provide information or click on any links within suspicious e-mails.

Although the Firm must be cautious about giving our customers specific advice, we may recommend that they contact law enforcement. We may also refer the customer to the Home Office Identity Fraud Steering Committee Web site listed in this guide.

Computer professionals may be helpful in counseling the customer on malware issues.

E-MAIL ETIQUETTE

When communicating with customers by e-mail:

- Be sure to include the customer’s name in the salutation.
- Use correct business language in accordance with our brand standard.
- Do not include any of the customer’s own confidential information such as social security number or account number.
- Make sure your message includes proper contact information.
- Never ask the customer to convey or confirm sensitive personal information through an e-mail.

AVOID GETTING “REELED IN”

Anyone who uses the Internet or e-mail should be aware of these common-sense precautions:

1. If you get an e-mail asking for personal or financial information, do not reply or click on any links contained in the e-mail.
2. Contact the business:
 - a. Open a new browser page and type the company’s URL in the address line or,
 - b. Call their official customer service phone number available on account statements or through the toll free number.
3. Keep your home computer’s anti-virus software up to date by downloading the most recent updates from the software company’s Web site. (T. Rowe Price updates your company computer’s anti-virus software for you on a regular basis.)
4. Monitor your banking and credit card statements carefully for unauthorized transactions.

