HIGHTOWER
Westchester

The 3 R's of Handling Phishing Messages

Phishing is a common scam where fraudsters trick you into sharing personal and financial information, such as usernames, passwords, credit card numbers, account numbers, and addresses. Scammers often pose as reputable companies in emails or texts to get you to reply or click on a link or attachment. This allows them to collect sensitive data, which they can use to make fraudulent purchases or steal your identity to open bank accounts, take out loans, or obtain medical care.

Falling for a phishing scam can have long-term consequences. However, with the right knowledge, you can avoid becoming a victim. Here are the three R's to follow when you receive a phishing message:

RECOGNIZE

When opening texts and emails that ask you to carry out an action such as clicking a link, calling a number, or downloading a file, you need to stop and scrutinize the message to see if any of the contents look off. Typically, the first sign that a message is not from the legitimate sender is by hovering over the email address or clicking on the contact's name. The sender's information will often have misspellings in the name or will include an email domain that the company doesn't use such as Gmail.com or Outlook.com. The body of the email may also include several spelling and grammar mistakes that a professional organization would likely have proofread.

examples

- You received an email from Amazon to update your billing address, but the email sender is, sarah@amazon-support.com.
- You received an unsolicited text from the U.S. Postal Service claiming that your package was delayed due to an inaccurate address.
- You received an email from Netflix asking to restart your membership after claiming the Apple Store or the Google Play store honored your request to delete your account.

RESIST

If you notice any of these red flags, resist the urge to interact further. Phishing messages often create a sense of urgency to get you to click on a fraudulent link. They might claim you've won something or that your account will be closed if you don't act quickly.

If you're unsure about the legitimacy of an email, contact the company directly using a website or phone number you trust.

REPORT

Before deleting the phishing message, report it to your phone or email provider. On your phone, press the "report junk" button within the message. In emails, right-click on the message and select "report phish" or "report scam," depending on your email provider. Block the sender to prevent future emails from the same address.

Additionally, notify the company being impersonated about the scam. Many companies have web pages for reporting fraudulent messages. They may issue a public announcement to warn others. You can also report the attempt to the Federal Trade Commission (FTC) and the FBI's Internet Crime Complaint Center (IC3) for further investigation.

conclusion

Phishing scams are a prevalent threat, but by following the three R's—Recognize, Resist, and Report—you can protect yourself from falling victim to these deceptive tactics. Always be vigilant when receiving unsolicited messages, and take the time to verify their authenticity. By resisting the urge to interact with suspicious content and promptly reporting it, you not only safeguard your personal information but also help prevent others from being targeted.

HIGHTOWER
Westchester

440 MAMARONECK AVENUE
SUITE 506
HARRISON, NY 10528
(914) 825-8630
HIGHTOWERWESTCHESTER.COM