



8 Tips to Avoid Email Phishing Scams

Provided by: Brady, Chapman, Holland & Associates

Every day, more than 3 billion phishing emails are sent out worldwide. These emails are tactics used by scammers to trick you into giving up sensitive information about you or your company. Here are eight tips to avoid phishing scams:



1. VERIFY THE SENDER'S EMAIL ADDRESS

Scammers may pretend to be your bank, a colleague or even a family member. Check any previous conversations with the sender or your address book to verify the email address.



2. LOOK FOR SPELLING ERRORS

Various spelling or grammatical errors within an email can indicate fraudulent activity.



3. NEVER GIVE OUT SENSITIVE INFORMATION

Most legitimate companies will avoid asking for personal information via email.



4. BE WARY OF URGENT MESSAGES

People are more likely to give up sensitive information when pressured by a sense of urgency.



5. CALL TO VERIFY REQUESTS

If you are skeptical of any requests made in an email, call the source directly to verify.



6. AVOID OPENING UNSOLICITED ATTACHMENTS

Attachments can be embedded with malware—if opened, malware can steal sensitive information by gaining access to your computer or network.



7. VERIFY HYPERLINKS

Before opening a hyperlink, hover over the link text to verify the linked web address.



8. CONTACT IT OR SECURITY TEAMS

If unsure of an email's validity, report it to your IT department or security team to have them check for fraudulent activity.