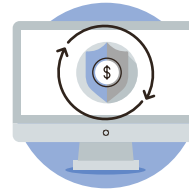
Six Key Guidelines for Email Security



Basic tips to protect your business, employees and customers from online attacks.

By Jeremy Stewart
Head of IT & Data Security, Strategic Financial Services, Inc.

OPEN WITH CARE - Do not open attachments from known or unknown sources that you are not expecting.

HOVER AND INSPECT - Always mouse over a link within an email to determine its destination is legitimate and matches the source of the email.

CONFIRM BEFORE CLICKING - If an email comes from a known source, but you are not expecting it, or it is just out of the ordinary, call the sender before clicking on a link or opening an attachment.

GO TO THE SOURCE - Use your web browser to go directly to any site that requires you to log in, do not access them through an email link.

DON'T TAKE THE BAIT - Companies usually do not send unsolicited email to verify your account information, nor do they request immediate action be taken or you risk the termination or suspension of your account. These are standard phishing tactics, delete the message immediately.

SEND SAFELY - When sending an email that contains PII (Personally Identifiable Information), use a secure email system such as Citrix Sharefile or Zix.

As the Head of IT and Data Integrity at Strategic, Jeremy oversees all aspects of the firm's technical infrastructure. He provides leadership for the continued enhancement and development of a robust and secure information technology environment throughout the firm. Jeremy is currently pursuing his Masters of Science in Cybersecurity.