VIP TECHNOLOGY
SOLUTIONS GROUP

HOW TO SPOT A PHISHING EMAIL

and avoid getting scammed

Phishing schemes have come a long way since the days of AOL. Make sure your team stays educated and aware of cybercrime in the evolving digital world.

EMAIL ADDRESS

Check the email address and domain for typos. Scammers will often register domains that are very similar to large corporations, but not exact. Look for misspellings, extra letters, numbers, or an additional word added to the domain.

Additionally, if legitimate companies have sent you emails in the past, most emailing platforms will keep a log of that information. Cross reference that email address with the one of the suspicious email.

DEAR CLIENT,

Often, scam emails will use a generic title such as "customer," "client," or "account user." You can bet that if you see any of these generic titles, the email is not from a legitimate source.

TYPOS

Legitimate companies hire professionals to write their emails. If you read through an email with more than one typo and it just doesn't make sense, mark it as fraudulent.

URGENCY

If an email is urging you to make changes to your account and threatening suspension, fines, or other negative consequences, it is likely phishing. Companies that depend on you for business shouldn't be pushy.

UNSOLICITED

If you have no reason to suspect any issues with your orders, accounts, or billing, then the email could be fraudulent. If you're not sure, contact the company directly from their site or give them a call.

LINK ADDRESS

Phishing emails are always going to try to route you to a fraudulent website to collect your information. The button or link within the email will look legitimate, but if you are using Google Chrome, hover over the link you can see in the lower left hand corner of your screen where the link is actually directing you.