# HOW TO SPOT A PHISHING ATTACK

Pay attention to details when evaluating an email to determine if it is a phishing scam. Generic greetings, typos, and poor grammar are good, but not foolproof, indicators of fraud. Other indicators include:

- The "From" name doesn't match the sending email address: "John Doe <william_s@yahoo.com>
- PORTIONS OF THE EMAIL ARE IN ALL CAPITAL LETTERS
- There are threats, dire warnings, and time constraints: "Your account will be blocked if you do not click the link below in the next 48 hours."
- The email is signed with a generic closing, such as "Customer Service"
- The sender's email address does not match the domain or organization the email purports to be from: Safelight Bank <william_s@yahoo.com>
- Immature requests from large legitimate organizations- such organizations would not ask you to help rebuild or confirm their database of customers
- Mismatched links in the email: "Please verify your Safelight account by clicking the link: secure.safelight.generic.com"
- Contact from a group that doesn't actually exist at your organization. If your IT emails come from "IT Support" and you receive a request from "helpdesk"
- Too good to be true offers- no one will send you a million dollars for a $1000 fee
- Direct request for a username and password
- A link in the email appears to point to a legitimate site but when hovered over or clicked, brings you to a completely different site.
- An email from a business or organization that you have no relationship with.
- Trust your instincts – If you think something isn't right, do not respond to or perform any action being requested in that email

SecurityInnovation®