Detecting a Phishing Email – Things to Watch For

1. Don’t trust the display name.

Just because it says it’s coming from a name of a person you know, or trust doesn’t mean that it truly is. Be sure to look at the email address to confirm the actual sender.

2. Consider that salutation.

Is the address general or vague? Is the salutation to “valued customer” or Dear [insert title here]?

3. Check for spelling errors.

Attackers are often less concerned about spelling or being grammatically correct than a normal sender would be.

4. Is the email asking for personal information?

Legitimate companies are unlikely to ask for personal information in an email.

5. Beware of urgency!

The emails might try to make it sound as there is some sort of emergency. For example, the CFO needs $25,000 wire transferred to [insert name here].

6. Look but don’t click.

Hover and mouse over links within the email without clicking on them. If the alt text looks strange or doesn’t match what the link description says, don’t click on it – report it.

7. Check the email signature.

Most legitimate sender will include a full signature block at the bottom of their emails.

8. Be careful with attachments.

Attackers like to trick you with an important attachment. It might have a long name. It might be posed as an overdue invoice.

9. Don’t believe everything you see.

If something seems slightly out of the norm, it’s better to be safe than sorry. If you see something off, then it’s best to report it to your IT department.

10. *When in doubt, contact IT.*

No matter the time of day, no matter the concern, most IT departments would rather you send something that turns out to be legitimate than put the organization at risk.

Primary
TITLE AGENCY, LLC

31800 Northwestern Hwy., Ste. 205
Farmington Hills, Michigan 48334

tel 248.702.0901 | fax 248.479.1771
State Lic. #0104114
www.PrimaryTitle.com