Rainier
MANAGED IT SERVICES

5 Red Flags of Phishing Emails: Think Before You Click

A single click can be the difference between maintaining data security and suffering massive financial losses. From the moment just one employee takes the bait in a phishing email, your business is vulnerable to data breaches and extensive downtime.

Quickly spot the red flags and put phishing emails where they belong:

1. Poor spelling and grammar

While occasional typos happen to even the best of us, an email filled with errors is a clear warning sign. Most companies push their campaigns through multiple review stages where errors are blitzed and language is refined. Unlikely errors throughout the entire message indicate that the same level of care was not taken, and therefore the message is likely fraudulent.

2. An offer too good to be true

Free items or a lottery win sure sound great, but when the offer comes out of nowhere and with no catch? There's definitely cause for concern. Take care not to get carried away and click without investigating deeper.

3. Random sender who knows too much

Phishing has advanced in recent years to include 'spear phishing', which is an email or offer designed especially for your business. Culprits take details from your public channels, such as a recent function or award, and then use it against you. The only clues? The sender is unknown – they weren't at the event or involved in any way. Take a moment to see if their story checks out.

4. The URL or email address is not quite right

One of the most effective techniques used in phishing emails is to use domains which sound almost right. For example, [microsoft.info.com] or [pay-pal.com]

Hover over the link with your mouse and review where it will take you. If it doesn't look right, or is completely different from the link text, send that email to the bin.

5. It asks for personal, financial or business details

Alarm bells should ring when a message contains a request for personal, business or financial information. If you believe there may be a genuine issue, you can initiate a check using established, trusted channels.

While education is the best way to ensure phishing emails are unsuccessful, a robust spam filter and solid anti-virus system provide peace of mind that your business has the best protection available.

Give us a call to discuss how we can secure your system against costly phishing attacks.