THE M&H MONITOR

SPAM: Treading Water in an Ever-Increasing Tide

By: Robert Demers

As we all know, spam is an unfortunate reality of email communications these days. One of the common tricks spammers use to trick people is to make their emails look like they came from an official source that a user would typically get email from. Examples are fake notifications from entities (Office 365, Wells Fargo, one's CFO, etc.) that try and coerce people to do something – wire money, open an infected attachment or click on a link that will bring them to a website that is either infected or trying to gather information. These emails are well disguised and can take a keen eye to discern against legitimate emails – they are even sending them to look like they are coming from company executives to try and fool people.

While there are many technological standards and protocols in place to combat this rising tide, it has and will remain a cat and mouse game. The tech industry will adopt a new method of identifying malicious or suspicious emails, and the spammer community will then try and find ways to circumvent them.

A few tips and tricks to help avoid the pitfalls these situations can bring:

1. Only open email attachments from people you know and are expecting to send you something.

Even if a sender is known, there is always a possibility they can be infected as well or their email account was compromised. If it looks OK and would be something they would send but it is not expected, a phone call would be best. Even emailing them in a separate email will not be 100% effective – we have seen cases where the spammer will actually reply back.

2. Never click on links in an email unless you know it is from a known good sender. If you are unsure, go to the page yourself outside of the link that was sent.

As mentioned above, many spammers try and impersonate legitimate businesses to try and get people to click their links.The links themselves may look official in the email itself, but the page you end up on could be infected or just malicious.Going directly to the website itself instead of going to a link

sent in an email will avoid using malicious links.

3.) Call or email M&H!

Last but not least, if ever in doubt please feel free to contact us here at M&H Consulting. We would be happy to take a look at any emails that look suspicious, or anything else that might come up at 866-964-8324 x1 or support@mhconsults.com

---

"It's not the most sophisticated Spam blocker I've tried, but it's the only one that works!"

TAKE $$$CASH$$$ FROM M&H CONSULTING

Refer a new Tech-For-A-Day client to M&H Consulting and mention this offer to us, and you will receive $25 for each PC the new client has. Call for details.