TJMicro Tech Tips

Keeping an Eye Out for Spam Emails

We've all received an email stating that a prince needs help and to please send money right away, and that you will be rewarded handsomely in the future. This email scam was very popular in the past, with unfortunately, many kind-hearted individuals falling victim to it. Nowadays, this email is very easy to spot and less people are tricked into sending money or providing their banking credentials. However, with the evolution of technology, spam emails have gotten harder to spot, and unfortunately we might not realize it is spam till it's too late.

Here are the top 3 types of scamming emails to keep an eye out for:

Phishing Emails

The sole purpose of these scam emails is to collect data or "phish" for your information. Phishing emails will often start off pretending that they are an official company, such as your bank, the government, or the organization you work for, and request you to confirm or reset your account information. Typically, it will request that you click a link which directs to a website that looks familiar – a mock-up of a bank or government website, usually. By signing into this fake site with your account credentials, they now have their hands on your information.

Compromised Account Emails

Some scam emails will look official, coming from a "trusted company" such as Microsoft or Apple, and indicating that your account or computer has been hacked. They usually then request that you download a file or click a link to help clean your system – when clicking that link downloads a virus onto your computer.

Extortion Scam

Although the previously mentioned scam emails usually attempt to appear helpful, the extortion scam emails focus on your fear of having something personal exposed, such as your credit card information or a personal videotape. These emails will demand for money, usually via e-transfer, in exchange for not releasing your personal information. However, in most cases, they do not have any of your information, and it's best just to not respond and delete these emails.

So, what do you do if you get one of these emails?

You want to get rid of these emails, immediately. Flag it as junk mail and permanently delete it from your email account. If the email was sent to your work email account, let your IT support know immediately. Odds are that you aren't the only person targeted in your company, and they need to get ahead of it before someone responds to the email, not realizing that it was spam.

What do you do if you opened the link or gave your information?

Firstly, inform IT support immediately so that they can start taking action. Be honest and open about what the scam was and what information you provided – this will allow them to be proactive about protecting your information.

If this happened on your personal laptop or account, you immediately want to run a full virus scan of your computer – most anti-virus software gives the option of running quick or full scans, and will manage any viruses found as it identifies them. Second, you want to change all of your passwords, prioritizing passwords for your most sensitive information, such as your bank account, or websites that have your credit card information stored. For the next little bit, you will want to monitor your accounts for any unusual activity.

How can you protect yourself?

1) Read each email you receive critically – whether or not it's from a known sender. If it seems out of character, contact the person using a different method (e.g. by phone, or at a different email address), as sometimes scammers will try to impersonate a known contact. Talk to your IT support team if you have any questions about the validity of an email.
2) Keep your anti-virus software update to date and run scans regularly on all of your devices.
3) Change your passwords frequently, and ensure that you are following protocol for a strong password.

As technology continues to evolve, we need to keep our guard up to protect our personal information and stay informed about new scamming strategies.

Kyle Hacker is the CEO of TJMicro Ltd – your complete source for professional IT services. Kyle has diverse experience in managing professional IT services and strives to meet the needs of all his clients. TJMicro Ltd provides tailored services to organizations of all sizes and across the private and public sector. To find out more about what TJMicro can do to help support your business, contact Kyle at kyle@tjmicro.com.

If you have any questions about how improve your email security or identify spam emails, please contact TJMicro Ltd by phone at 416-317-6000 or email at info@tjmicro.com.

To find out more about services offered by TJMicro Ltd, visit us at www.tjmicro.com.

TJ MICRO

Your complete source for professional IT services