September 2021

TIPS TO IDENTIFY PHISHING EMAILS

Cyberattacks are on the rise everywhere, including in Ontario. Health care is a particularly lucrative target for hackers who prey on busy clinicians who may not be aware of the latest scams and how to protect themselves against these malicious threats. One of the most common cyberthreats is phishing. Phishing is a cyberattack by email designed to try and steal information from individuals online.

OntarioMD (OMD) has put together a list of 10 tips to keep your personal information and your patient data safe from phishing attempts.

1. Unfamiliar Tone or Greeting

Often in phishing attempts, the person who is trying to phish will try to act like someone you communicate with regularly (i.e., a colleague or a boss). Pay attention to things like the greeting in the email – is it similar to how you are usually addressed by that person? The tone and language used in the email can also be good indicators of a phishing attempt.

2. Grammatical and Spelling Errors

Most of the email servers today have built-in spell check, so if you receive an email that has lots of spelling and grammatical errors, you've likely received a phishing email. Ask yourself: Does the language make sense and does the sentence structure in the email make sense? When using email in a work setting, we expect that emails are written and delivered in a professional manner, therefore, content that doesn't fit that expectation should be questioned.

3. Suspicious Email Address

Suspicious email addresses are easy to spot if you know what to look for. If the email address domain has used periods or hyphens to separate words (for instance, ont.ariomd.com), this could be a sign of a phishing attempt. The hacker is trying to make the domain look normal at first glance, but when inspected, you notice the extra period in the email domain name. Hackers also try to disguise their email addresses. An email may appear to be from Amazon, for example, but if you hover over the address or right click on it, you may see an email address that is not in fact from Amazon. This is a cause for suspicion. It's better to be safe than sorry and not respond to the email.

4. Suspicious Links

In the body of an email, it is common for hackers to try and hide suspicious links by embedding them into the body text. If you receive an email that has an embedded link, hover your mouse over the word and the link will appear. Does the link appear to be a legitimate, or does it look suspicious? Does the domain name match the sender? Is the spelling correct in the domain name? Make sure you are confident in the safety of the link before you click it.

5. Urgent Action Required

Instilling a sense of urgency in the email is a tactic often used to try and have the recipient take immediate action without considering the request or examining the sender. If you receive an urgent request by email, take the time to review the authenticity of the sender and consider if what they are urgently requesting is reasonable.

6. Suspicious Attachments

If you receive an email that has an attachment, before opening it, ask yourself if have you requested or were expecting one in this email? Attachments are a common way for you to get hacked and for malware to enter your system. The following attachment extensions are commonly associated with malware downloads: '.zip', '.exe' and '.scr', so if you receive an attachment with any of these, it could be a phishing attempt. If the attachment is a Microsoft Office file ending in an 'm', this is an indication that the file contains code and may also be a phishing attempt. Err on the side of caution and do not open suspicious attachments.

7. Strange Requests

There are many types of requests that could potentially be phishing attempts, for example:

Not the Norm: If an email asks you to follow a link to an internal company survey, but the sender of the email is not who you expect, verify the legitimacy of the email before following the link.

Confidential Request: If the sender emphasizes the request you have received is confidential, this is likely because they don't want anyone else to identify the request as a phishing attempt.

Requesting Personal Information: If you receive an email that requests personal credentials (name, address, banking information, etc.) avoid clicking any links. Companies are not likely to send you an email request for any personal credentials and this is likely a phishing attempt.

8. Email Length

In some cases, phishing emails are strategically composed to be very short so that the ambiguity of the message will lead the recipient into clicking any links or attachments. In these cases, ensure that you inspect who the sender of the email is. *Please remember tip 3 above – Suspicious Email Address*.

9. Unsolicited Email

When the email you receive is unexpected, always proceed with caution. If you do not remember subscribing to something or asking a company for information, be wary. A company will not send you emails unless you have given your permission to receive their emails.

10. Great Offer

If you receive an email with an offer that seems too good to be true, it's probably because it is. Emails like this could claim you are the recipient of a large monetary prize or the winner of an all-expenses-paid family vacation. Did you enter a contest? Do you know the sender? Be careful when these emails are received. Even if you know the sender, be wary of the email's content because you don't know if your friend or colleague has been hacked themselves and the hacker is using their email to attack the person's network of friends.

Need Help?

When determining whether an email is a potential phishing attempt, you should consider all the above guidelines and use your best judgement to apply them to your specific situation.

If you want to learn more about Privacy, Security and how to protect yourself and your office, OMD offers two complimentary online **Privacy & Security Training Modules** designed specifically for health care professionals. One covers standard privacy and security principles and best practices, and the second module covers considerations when using virtual care tools.

If you have more questions about privacy and security, using digital communication and other practice tools, OMD is at your service. Contact us at support@ontariomd.com and we will be happy to answer your questions.