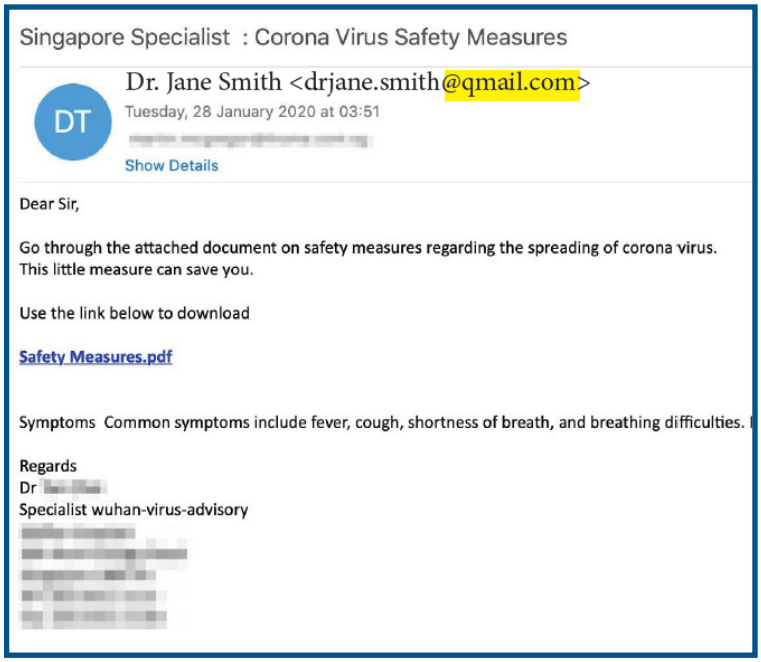
Health Industry Cyber Security Practices:
Managing Threats and Protecting Patients (HICP)

Social Engineering Attacks

What are Social Engineering Attacks?

One common type of social engineering attack is called "phishing," which is an attempt to trick you, a colleague, or someone else in the workplace into giving out information using email. An inbound phishing email includes an active link or file (often a picture/graphic, statement, or invoice). The email appears to come from a legitimate source, such as a friend, coworker, manager, company, vendor, or even the user's own email address. At times, the email address could be identical, except for one letter such as "qmail" instead of "gmail." Clicking to open the link or file takes the user to a website that may solicit sensitive information or proactively infect the computer. Accessing the link or file may result in malicious software being downloaded or access being provided to information stored on your computer or other computers within your network.


Singapore Specialist : Corona Virus Safety Measures

DT

Dr. Jane Smith <drjane.smith@qmail.com>

Tuesday, 28 January 2020 at 03:51

Show Details

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus. This little measure can save you.

Use the link below to download

Safety Measures.pdf

Symptoms Common symptoms include fever, cough, shortness of breath, and breathing difficulties.

Regards

Dr

Specialist wuhan-virus-advisory

Real-World Scenario:

Members of your workforce receive a fraudulent email from a threat actor disguised as an IT support person from your patient billing company. The email instructs your employees to click on a link to change their billing software passwords. An employee who clicks the link is directed to a fake login page, which collects that employee's login credentials and transmits this information to the attackers. The threat actor then uses the employee's login credentials to access your organization's financial and patient data. This can cause damage to your network while also gaining further access to your enterprise, sometimes even taking control or stealing patient data.

Impact

Phishing attacks can compromise health information of patient's names, dates of birth, medical record numbers, and Social Security numbers. A health system provided notice of an October 2021 healthcare data breach that exposed PHI and resulted in data exfiltration. A submission to the Office of the Attorney General revealed that the breach impacted 1,357,879 individuals. This information could have been sold to other threat actors for purposes such as identity theft. These attacks not only impact a health organization's bottom line, but also impacts their reputation and the possibility for interrupted care delivery.

How Can HICP Help?

The publication, Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP), aims to raise awareness, provide vetted cybersecurity practices, and move towards consistency in managing the current most pertinent cybersecurity threats to the sector. The material on this flyer is a section of the publication that examines cybersecurity threats and vulnerabilities that affect the healthcare industry.

Staying Resilient to Phishing Attacks

On average, a person will receive a large number of emails per day. Knowing which are safe to open can get tricky if you are not asking yourself the following questions:

- Do I know the sender?
- Are there any spelling or grammatical errors or any other indicators that the tone or style of the email is off?

- Beware of emails that are familiar that may be compromised; is the email expected/does it make sense from the sender?
- Before clicking on a link, did I hover over it to identify the website address?
- Are you suspicious of the email? If in doubt, do NOT open any attachments.
- What are my organization's processes for reporting suspicious emails? If in doubt- call your HelpDesk/IT Support or administrators.

When To Ask About E-Mails

Familiarize yourself with your organization's policies for reporting a suspicious email regularly so you are prepared when you need it. Whenever you receive an email that sounds too good to be true or that you were not expecting, verify it before opening it!

Check with colleagues to find out whether they received the same phishy email. You can always seek the guidance of your IT security support team or similar point of contact. Talk to them to find out whether your account is protected with the proper security filters to ward off unwanted junk mail.

How Can You Mitigate Social Engineering Attacks?

Each individual threat discussed in the HICP publication provides threat specific mitigation practices. The table below lists the phishing mitigations along with a quick reference key to help locate further information in the HICP documents. The mitigation practices are covered in greater detail in the technical volumes included in the publication: Technical Volume 1 for Small Organizations and Volume 2 for medium and large organizations.

Social Engineering Attacks Mitigation Practices to Consider
Be suspicious of emails from unknown senders, emails that request sensitive information such as Protected Health Information (PHI) or personal information, or emails that include a call to action that stresses urgency or importance **(1.S.B)**
Train staff to recognize suspicious e-mails and to know where to forward them **(1.S.B)**
Never open email attachments from unknown senders **(1.S.B)**
Tag external emails to make them recognizable to staff **(1.S.A)**
Implement incident response plays to manage successful phishing attacks **(8.M.A)**
Implement advanced technologies for detecting and testing e-mail for malicious content or links **(1.L.A)**
Implement multi-factor authentication (MFA) **(1.S.A, 3.M.D)**
Implement proven and tested response procedures when employees click on phishing e-mails **(1.S.C)**
Establish cyber threat information sharing with other healthcare organizations **(Main Document Page 20)**

Key: 1-10 = Cybersecurity Practice | S = Small (Tech Vol 1) | M = Medium (Tech Vol 2) | L = Large (Tech Vol 2) | A-Z= Respective Sub-Practice

Example: "1.S.B Education": "1" refers to the cybersecurity Practice "Email Protection System" | "S" refers to Small size organization | "B" refers to the sub practice for small size organization within the Email Protection System – Cybersecurity Practice, which in this case is "Education"