

October 20, 2017

The Commonwealth has recently experienced an increase in the number of social engineering incidents where hackers have attempted to solicit sensitive information from Commonwealth staff through deceptive emails and phone calls.

You play a critical role in maintaining a secure environment and protecting the Commonwealth’s sensitive information, assets, and reputation. Opening an email that contains malware can lead to an agency having to shut down part of its business for days - even weeks - and a significant loss of productivity. It is vitally important that you understand how to identify and respond to social engineering and phishing attempts.

Deception is a hacker’s most powerful tool, so you need to be constantly aware of the threats that you will encounter through technology, over the phone, or in person. It is important to recognize that attackers will not only try to hack directly into the Commonwealth network but will also try to lure you into unwittingly giving them access.

**You will encounter these types of threats, and no IT organization can prevent them using technology alone**.

EOTSS will be providing Commonwealth-wide cybersecurity awareness training in 2018. In the meantime, please review the following guidelines carefully.

**What is Social Engineering?**

Social engineering involves obtaining confidential information from individuals through deceptive means by mail, email (also known as phishing), over the phone, and increasingly through text messages.

*How can you identify a social engineering attempt via email?*

Here are some red flags to watch out for:

Appearance

* Grammatical errors or misspellings
* Low quality or disorganized graphics or logos
* A generic greeting instead of your name

Sender’s Identity

* Sender’s name does not match email address
* Sender’s email domain does not match the company the party claims to represent
* Email domains read from right to left. @boston.gov is the email domain for the City of Boston. @boston.hackers.com is not.

Message / Tone

* Phishing attempts will often involve demands and language requiring urgent action to get you to react.
* Requests can include opening an attachment, clicking a link, or providing sensitive information.
* Be cautious of emails that warn that “your account will be closed” or “there was an unauthorized login attempt”.
* Never reply to an email with your account information or password.
* If an email includes a link that asks you to “click here to change your password” it may not be legitimate.  Instead of clicking the link, open your browser and manually type in the address of the web site.

As hackers have become more sophisticated, their phishing emails have started to look more professional. Be extra careful.

If you have any doubts about an email, before responding or clicking on a link, check with the CommonHelp Service Desk by emailing CommonHelpServiceDesk@state.ma.us, calling (866) 888-2808, or opening a Service Request at <https://massgov.service-now.com>.

*How can you identify a social engineering attempt via phone?*

Red flags to watch out for include:

Caller’s Identity

* Caller refuses to provide contact information or complete employee information
* Caller name-drops or mentions internal technologies or initiatives

Request / Tone

* Requests proprietary, non-public or personal information
* Intimidates or pressures to provide information quickly

As with e-mail, you should never provide your formal identification or sensitive information in response to a phone solicitation.

**How should you respond?**

In the case of a suspicious email:

* Do not respond to emails or text messages asking for confidential or personal information.
* Do not open attachments or click on links within suspicious emails from an unknown individual.
* Limit details disclosed in “out of office” messages.

In the case of a suspicious phone call:

* Verify the caller’s identity. Ask for their name and agency and then confirm the information on Mass.gov or through the Global Address Book in Outlook.
* Take their name and call them back using independently verified contact details (not the contact details provided by the caller).
* Never provide personal information, details of other employees, or disclose other non-public information about the Commonwealth unless authorized *and* you are certain about the caller’s identity.
* Never reveal sensitive or other internal information to unknown individuals on the phone.
* Do not feel pressured into sharing information by a caller using intimidation techniques.

Once again, if you suspect any questionable activity, report it immediately to your manager and the CommonHelp Service Desk at CommonHelpServiceDesk@state.ma.us, by phone at (866) 888-2808, or by opening a Service Request at <https://massgov.service-now.com>.

By following these simple steps, you will avoid providing a hacker access to the Commonwealth’s network or compromising sensitive organizational, client, or personal data.

If you have any additional questions, or would like to learn more about how Technology Services & Security is working towards securing IT data and infrastructure throughout the Commonwealth, please email Chief Technology and Security Officer Dennis McDermitt at Dennis.McDermitt@mass.gov, or Deputy Chief Technology Officer John Merto at John.Merto@mass.gov.