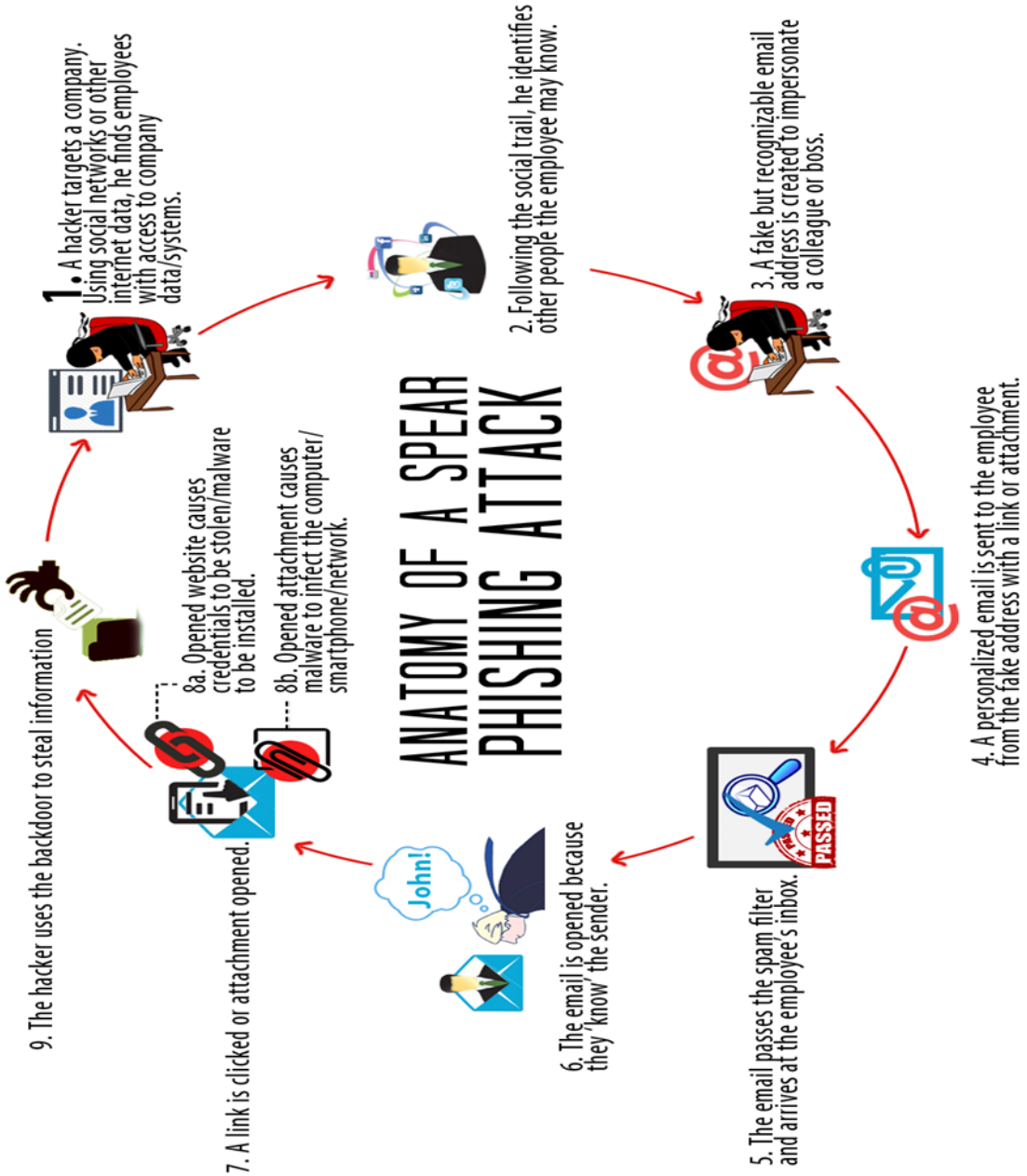


DAS/BEST

Phishing Quick Response Guide

IT Security Division – Cyber Security Awareness

The mission of the Cyber Security Awareness team is to spread awareness to our computer users through training & education on the best practices when utilizing the State of Connecticut network infrastructure.

http://www.ct.gov/bestservices/cwp/view.asp?a=4063&q=476440

DAS/BEST Helpdesk 860-622-2300

Prepare

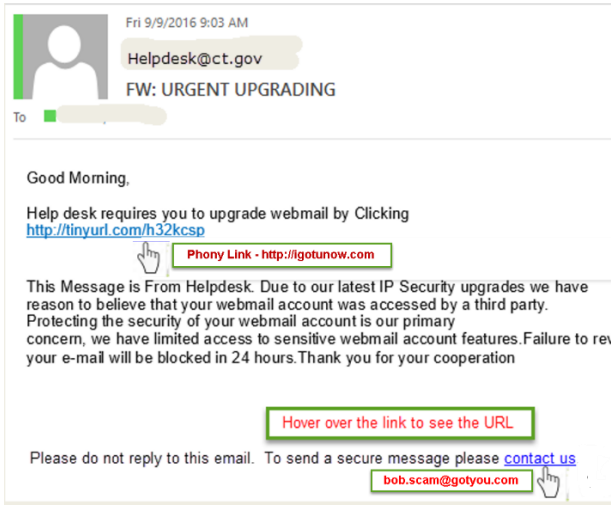
Know what to look for

Step One - Complete the Security Awareness Training offered by your agency.

Review the DAS/BEST Phishing Presentation http://www.ct.gov/bestservices/cwp/view.asp?a=4063&q=585736

Signs of a Phishing attempt:

> "From" field of an email can be easily faked (spoofed). It might appear completely correct, or have a similar variation. account_security@mypay.com
>
> On the other hand, the message may come from a legitimate email account, because that account has been compromised. john.smith.yourboss@ct.gov
>
> *This can occur when the attackers obtain someone's login credentials and email contacts in their address book in order to obtain more accounts.*



Other recognition factors of phishing attempts:

> *1) Generic Greeting*
>
> *2) Fake Sender's Address*
>
> *3) False Sense of Urgency*
>
> *4) Fake Web Links. Deceptive Web Links. Email is requiring that you follow a link to sign up for a great deal, or to log in and verify your account status, or encourages you to view/read an attachment. (Hover over the link to view the URL that it redirects to.)*
>
> *5) Emails that appear like a website*
>
> *6) Misspellings and Bad Grammar*

Prevent

Don't become a victim

Be cognizant and vigilant of this threat.

Before clicking on any web link within a message or opening up an attachment, be sure the source of the email is legitimate. Contact the sender via phone if necessary.

The links and attachments can contain malware, spyware, viruses, and Trojan horses

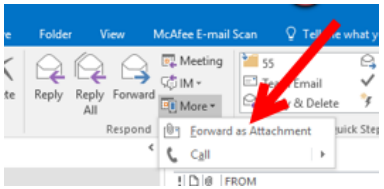
If you click on these illegitimate links/attachments, your computer or account will likely be compromised

Respond

Action to take

Remember SPAM is not Phishing. SPAM is unwanted but not malicious. SPAMMERs are not trying to acquire sensitive info. If there are suspicious links or attachments (see first panel), consider it a phishing attempt. SPAM can be deleted.

Forward any suspected phishing emails to BEST.PhishingAlert.Submission <BEST.PhishingAlert.Submission@ct.gov>
Use the subject line of 'Phishing Attempt Notification'.
Highlight the email within your Outlook inbox. Select More then Forward as Attachment.



Enter the email above in the To… line.

Or

In outlook select file > save as, name the file and select save. Attach to the email you are forwarding to BEST. Delete the email once it has been forwarded.

Recover

A link or attachment was selected

If you have selected a link or opened an attachment before you realize it was a phishing attempt, remove the device from the network and contact your Desktop Support group immediately. Do not shut the device down, as the ITSecurity group may want to take a memory capture.