COVID-19 Phishing Scams

COVID-19, coronavirus and related words/topics are being used by cybercriminals as a theme for phishing attempts. Also, the emails will be branded and formatted in such a way to resemble trusted organizations, such as the World Health Organization (WHO) or Center for Disease Control and Prevention (CDC).

Prevention

1. **Unsolicited Emails**: Avoid clicking on links and opening attachments from unsolicited emails.
2. **Trusted Sources**: Go to the trusted websites yourself; do not click on links.
3. **Charity**: Verify the authenticity of charities yourself.
4. **MEL’s Email Dos & Don’ts**: Send these four tips and the MEL infographic (attached) to all individuals with access to your network.

Resources

Check out NJCCIC’s bulletin on COVID-19, along with tips for teleworkers working from home:  
https://www.cyber.nj.gov/be-sure-to-secure

Here are the trusted sites referenced above for WHO, CDC and FTC’s Charity page:  
https://www.consumer.ftc.gov/articles/0074-giving-charity
EMAIL ADDRESSES
- Do you recognize the sender and the CCs?
- Is the sender’s email spelled correctly? (i.e. “YourMayor” vs. “YourMay0r”)

DATE & TIME
- Was the email sent on a typical day and at a typical time?

EMAIL CONTENT
- Are the format and grammar in the email typical for the sender?
- Does the content seem atypical?
- Did the sender seem overly urgent?
- Does the email ask for person info/login info?

SUBJECT
- Is the subject a typical style for the sender?
- Does the subject match the email content?

ATTACHMENT
- Is an attachment needed for the email content?
- Were you expecting the attachment?
- Is it a “.txt” file?

LINKS
- Does the link look appropriate?
- Does the web address match the hyperlink shown (scroll over the hyperlink)?

DON’T GET PHISHED!
... but if you do, remember to
1. Report to Claim Administrator
2. Call XL Catlin 24/7 Breach Hotline at (855) 566-4724 and they will triage your incident.