To: Signet Jewelers Team Members

From: Scott Lancaster, SVP, Chief Information Security & Privacy Officer

Date: March 17, 2020

Subject: Email phishing reminders to keep Signet's information safe

Our thoughts are with everyone who has been affected by the coronavirus during this uncertain time. But despite that uncertainty, our purpose remains the same — to keep our customer's, team member's, vendor's, and company information assets safe.

At a time like this it may seem silly to be worrying about phishing emails, but this the most opportune time for people to prey on our fears – and phishing is a great way to catch us off-guard.

Phishing emails are emails that appear to be official communications from a trusted source. They might ask you to verify or provide personal information through a link in an attachment in the email, or they may request you take other specific actions. All team members and contractors are responsible for safeguarding Signet's information assets – **don't fall victim to these attacks**.

Emails about Coronavirus - At this time - ignore any Coronavirus messages that originate from messages tagged with the External Email: Please use caution. The only messages that are legit are either internal or from a trusted third party.

What to do

Be aware that there are several forms of phishing, know what to look for, and how to respond when you receive a suspicious email. As attacks become more sophisticated, stay informed and aware.

- **To identify a phishing attempt, look for:**
  - Emails sent by unexpected parties that you do not normally interact with
  - Email addresses that do not appear to come from our internal system (*see more on email tags below*)
  - Inconsistent hyperlink information (display name and actual URL address are not the same)
  - Spelling and grammatical errors
  - Generic or unusual greetings
  - An extreme sense of urgency

- **Use Signet's email headers to help you identify potential threats.** All emails originating *outside* the Signet Jewelers email system automatically add one of the following tags:
  - ***External Email: Please Use Caution*** – external emails appearing to be internal are a serious threat
  - ***Signet Partner: Trusted Sender*** – examples include Workday, Service Now and credit partners

- **Report the suspicious email** by contacting the IT Corporate Service Desk (ITCSD@signetjewelers.com or 844-550-5578) to open a ticket.
  - When providing a sample of a suspicious email, create a new email message and attach a copy of the suspicious email – this preserves the email header information needed to do research.
  - Do NOT simply forward it as the email header information needed for research will be lost.

Thank you for your help in keeping Signet secure for our team members and customers.