GRAHAM COMPANY

MARCH 20, 2020

COVID-19: ADDRESSING CYBER SECURITY RISKS

As COVID-19 spreads around the globe, organizations should be aware of the increased risk of cybersecurity and privacy incidents that could lead to ransomware infections, business email compromise, or compromise of information that may be protected under state, federal, and international privacy laws.

COVID-19 Phishing Attacks

The ongoing pandemic has provided cybercriminals with an opportunity to seize on the widespread uncertainty. Phishing emails have already begun, and some examples include using subjects such as:

- **Live Map Websites**: Some phishing emails use a live map website that shows the spread of coronavirus as a way of spreading malware.
- **Vaccination and Medication**: Scammers may promise access to a special vaccine; however, experts estimate that it will take over a year to create one.
- **Offers for Hard to Find Items**: Phishing emails will offer "too good to be true deals" on surgical masks and other medical equipment not easily available for purchase.

When seeking information about the coronavirus, it is best to visit the CDC website.

Identifying a Phishing Email

Cybercriminals have become extremely sophisticated and skilled at crafting

realistic emails. Individuals should scrutinize any email, text, or social media post related to COVID-19. Stop and consider if the email “looks right”. If something feels wrong - don’t open it. It is important to consider the following:

1. **Is the email expected?** An unsolicited or otherwise unexpected and unusual email may be part of a phishing attack.
2. **Does the sender’s address look right?** If the sender’s email address is misspelled or uses an unusual domain, it is coming from a completely different email account.
3. **Does the body of the email seem legitimate?** Check for misspellings, grammatical errors, and stylistic discrepancies.
4. **Do links point where they should?** Hover over links and check to see if the target address points to where you expect.
5. **Does the email evoke a sense of urgency?** Cybercriminals use urgency to bypass peoples’ mental filters.
6. **Does the email request sensitive information?** If so, it is probably a phishing email, and you should not respond or click on any links.

We urge you and your employees to use extra caution when accessing information to stay up to date on COVID-19 developments. Feel free to reach out to any member of your Service Team with questions.

For additional COVID-19 resources and risk management recommendations, please visit our **COVID-19 Risk Management Center**.

A PDF of the above information can be found **here**.