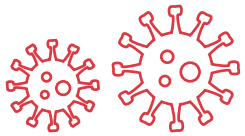
CYBER RISK IN RELATION TO COVID-19



Issue:

New phishing attempts

Cyber thieves are using the recent developments surrounding the novel coronavirus (COVID-19) as an opportunity to send phishing emails and spread malware attacks. Most recently, we've seen phishing emails impersonating the U.S. Centers for Disease Control and Prevention (CDC), the World Health Organization (WHO) and other health authorities. An example is a phishing email that specifically tricks users into downloading and running a malicious application that, while showing a coronavirus map loaded from a legitimate online source, in the background is collecting credit card numbers, login credentials and various other sensitive information.

Consideration:

Look for these red flags and follow these steps if you suspect an email or phone call is a potential phishing attempt:

- Unsolicited communications, especially from organizations or companies with whom you have no relationship.
- Requests for transactions such as direct deposit or electronic funds transfer.
- Requests with an overwhelming sense of urgency, or asking you complete an attached document immediately.
- Requests for your username and/or password, or other personal details such as banking information or log in credentials.
- Links that don't match: roll your cursor over the link and see if the link that pops up is consistent with the email address and message content. If not, don't click.
- Always independently verify that the source of emails or phone calls requesting information or providing wire transfer instructions is legitimate and that people are who they say they are.

Issue:

System stress and confidentiality

When employees work from home, there may be strains on the company's network and additional remote issues to consider.

Consideration:

Consider the following tips for your employees to help maintain network security and performance while working remotely:

- Limit use of large email attachments and other programs that will put additional pressure on your company's network bandwidth ecosystems.
- Unplug Alexa/Google or any other device that can "listen in" while you're on Skype calls to avoid the potential for sensitive company information (e.g., account numbers, company plans, etc.) to be compromised.
- Do not forward emails that contain attachments, highly restricted or company confidential content to personal email accounts as it potentially exposes your company to the unintentional disclosure of this information.
- Avoid reading, talking about, or leaving confidential or highly restricted company information in any unsecured work-from-home area.
- Lock or logoff and secure your work device when not in use.
- Shred documents with sensitive information as appropriate.
- Restart your machine daily.

THE HARTFORD

Business Insurance
Employee Benefits
Auto
Home