With businesses transitioning into a remote work environment, cyber risks will naturally increase. Below you will find an Evolve email template addressing best practices to avoid a cyber incident & examples of cyber-attacks exploiting the spread of COVID-19. Please feel free to adjust the template as needed.*

Client Advisory: COVID-19 Cyber Attacks

Dear Evolve Customers,

Given recent events, it is our responsibility to keep you informed about how the COVID-19 Coronavirus epidemic has impacted businesses from a Cyber perspective.

Since the start of the new year, Cyber criminals have registered over 4,000 domain names containing the phrases "Corona" and/or "Covid". These domains are being used to execute phishing and ransomware attacks disguised as Coronavirus related emails. Fraudulent emails may come in the form of a message from the Center for Disease Control & Prevention (CDS), health advice from a medical specialist, or even internal workplace policy notifications. **Click here to learn more.**

Best Practices to Avoid a Cyber Incident

Since many businesses are instructing staff members to work remotely to mitigate the spread of COVID-19, the chances of companies experiencing a cybercrime incident, such as a phishing scam or ransomware attack, have increased dramatically. Here are some helpful practices that you can utilize to avoid falling victim to these attacks:

1. **Multi Factor Authentication:** In order to prevent hackers from obtaining access to emails, we highly recommend utilizing **Multi-Factor Authentication (MFA)** when logging into email related accounts and applications that require a username and password. MFA will send a text / alert to the user's cell phone with an authorization code, which will be used to confirm the person logging into the email account is in fact them. This is one of the most successful methods of preventing hackers from using brute force attacks, in which they run a program that rallies through a series of passwords until one works.

2. **Phishing Training:** One of the best practices that businesses can employ in order to prevent fraudulent email incidents is to train personnel on how to spot them. If you are an Evolve policyholder, you have access to one of our free risk management tools called **CyberRiskAware**. This program allows the user to create fake phishing email campaigns which are sent to staff members. If a staff member opens the email and clicks on a link, they will be prompted to watch an educational video about fraudulent email awareness.

3. **Advanced Preparation / Anticipation:** In the event of a phishing or ransomware attack, it is important to have a plan of action in place in order to contain the incident as quickly as possible. Our 24/7 cyber incident response team is ready to provide immediate assistance, so please be sure to contract them as quickly as possible if you believe your business may have experiences an email breach.

Recently Reported COVID-19 Hacks

Click the links below for more information on targeted COVID-19 hacks in recent news:

- **Hospital for Special Surgery (HHS)**

- Health and Human Services Department
- Princess Cruises