Coronavirus (COVID-19) IT Updates

Cybersecurity Exploitation of COVID-19

The Ethos IT team would like to ensure everyone remains vigilant around IT security in this time of crisis surrounding COVID-19.

With the increase of people working from home, malicious actors are seeking to exploit the situation and are increasing their overall efforts around phishing attacks, scams and malware infections. These campaigns have become quite sophisticated in the use of legitimate data to draw in attention to their fraudulent links, websites and attempts to gather sensitive data.

The Department of Homeland Security CISA (Cyber and Infrastructure) are warning individuals to remain vigilant for scams related to Coronavirus Disease 2019 (COVID-19) after the U.S. Health and Human Services Department suffered a major cyberattack.

Cybersecurity Best Practices

Here are just some of the guidelines to follow to best protect not only Ethos but also yourself.

1. Don't open email from unknown senders and click on unknown links in email. Attackers are using COVID-19 to spread malicious content in some cases using real information to gather attention to their scam.

2. Ensure your anti-virus is installed, working and up to date on your computer. While we primarily focus on the Ethos IT managed software, this also applies to any personal devices you have on your home network that can come into contact with your Ethos-owned device.

3. Ensure your home Network equipment is secure and up to date. Change all default passwords for both your Wireless SSID but also your administrative access to the device.

4. Connect to the VPN (*Ethos Remote Access Network*) only when specifically necessary to access Ethos restricted resources such as file shares, ADP and so on.

5. Utilize your Ethos-issued device for business purposes only. Personal use of business equipment is prohibited and can increase the risk of infection through these additional activities.

6. Be aware of ongoing IT security alerts best practices by following ongoing news around this topic.

7. Should you receive an email, notification, or piece of digital correspondence from a source you are not familiar with please contact the IT department via the ticket system.

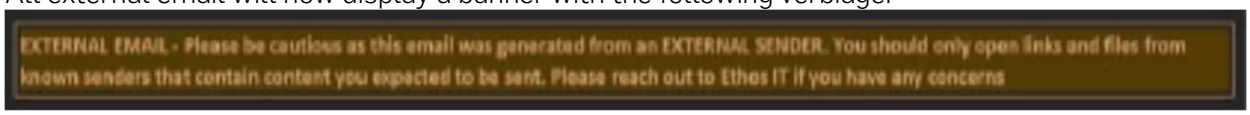
Information Technology Security Initiatives

Here are some initiatives we have put together to further protect Ethos.

1. Email filtering and protection will be increased to further identify and block email containing malicious content such as spam, phishing and malware content.

2. Endpoint Protection will be upgraded, where not already done, to an enhanced endpoint protection agent.

3. All external email will now display a banner with the following verbiage:



4. Firewall security policies and review will be increased.

5. Continuous efforts will be made by Ethos IT to enhance our protections

Updates

The Ethos IT team will continue to monitor and adapt to the ever-changing cyber security landscape not only as it pertains to COVID-19, but also as it pertains to the ongoing nature of threats that exist on a continuous basis. As always please reach out to IT by submitting an Autotask IT Ticket for further assistance.