TechTips Newsletter

tech hero

Insider Tips To Make Your Business Run Faster, Easier And More Profitably

May 2020

This monthly publication provided courtesy of Nina Tran, Cyber Security Manager, Tech Hero

Our Mission: To build a community of successful minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

Hurricane 2020 Preparedness During The COVID-19 Pandemic

As you continue to take precautions to keep yourself and your family safe from the coronavirus (COVID-19) pandemic, it is important to stay prepared for other disasters. Hurricane season begins on June 1, and the time to prepare is now.

FEMA continues to coordinate with state, local, tribal, and territorial officials, along with the private sector, to share operational guidance and to encourage hurricane planning that reflects public health guidelines. While many preparedness tools available to you are the same, certain actions may look different while COVID-19 remains a concern. FEMA has updated guidelines for preparing for hurricane season.

Know Your Evacuation Route

Check with local officials about updated evacuation shelters for this year. You should note that your regular shelter may not be open this year due to COVID-19. If you evacuate to a community shelter, follow the latest guidelines from the Centers for Disease Control and Prevention (CDC).

If you are able, bring items that can help protect you and others in the shelter from COVID-19, such as hand sanitizer, cleaning materials, and two cloth face coverings per person. Children under 2 years old and people who have trouble breathing should not wear cloth face coverings. While at the shelter, be sure to wash your hands regularly. If possible, be sure to maintain a physical distance of at least 6 feet of space between you and people who aren't members of your household.

Gather Supplies

Have enough food, water, and other supplies for every member of your family to last at least 72 hours. Consider what unique needs your family might have, such as supplies for pets or seniors and prescription medications. In addition, it is recommended that you add two cloth face coverings per family member and cleaning items to your kit, like soap, hand sanitizer, disinfecting wipes, or general household cleaning supplies to disinfect surfaces. After a hurricane, you may not have access to these supplies for days or even weeks. Preparing now ensures that you are well-equipped to stay safe if you need to quickly grab your go kit and evacuate to a community shelter.

As you prepare, be mindful that not everyone can afford to respond by stocking up on necessities. For those who can afford it, making essential purchases in advance will allow for longer time periods between shopping trips and help to protect those who are unable to procure essentials in advance of the pandemic and must shop more frequently.

Make an Emergency Plan

Make sure everyone in your household knows and understands your hurricane plan. Discuss the latest CDC guidance on COVID-19 and how it may affect your hurricane planning. Don't forget a plan for the office, kids' daycare, and anywhere you frequent.

Download the FEMA mobile app

Download the FEMA mobile app for disaster resources, weather alerts, and safety tips. Available in English and Spanish, the app provides a customizable checklist of emergency supplies, maps of open shelters and recovery centers, disaster survival tips, and weather alerts from the National Weather Service.

Author: Carlos J. Castillo, Acting Deputy Administrator of Resilience

The coronavirus (COVID-19) pandemic has forced many workers to rely on remote solutions to do their jobs. In particular, video conferencing services like Skype and Zoom have seen an astronomical rise in usage. In tandem with this, phishing campaigns targeting remote workers have also seen a large increase. This is proven true with a particularly convincing phishing campaign making the rounds right now.

According to a blog post from Cofense, a company that specializes in phishing attack mitigation, there is a new campaign looking for Skype credentials. The attack is so convincing for the following reason, according to Cofense's Harsh Patel:

For this attack, the threat actor created an email that looks eerily similar to a legitimate pending notification coming from Skype. The threat actor tries to spoof a convincing Skype phone number and email address in the form of 67519-81987[@]skype.[REDACTED EMAIL]. While the sender address may appear legitimate at first glance, the real sender can be found in the return-path displayed as "sent from," which also happens to be an external compromised account. Although there are many ways to exploit a compromised account, for this phishing campaign the threat actor chose to use it to send out even more phishing campaigns masquerading as a trusted colleague or friend. These phishing attacks have been able to bypass services like Proofpoint and Microsoft's 365 EOP, meaning they are convincing enough to not get flagged as malicious. Since this is the case, it can make sense why some individuals, especially in these uncertain times, would fall victim to the attack. Times of high stress and a total social upheaval of what many deem to be normal can cause bad decisions.

The question remains, however, why would an attacker want Skype credentials in the first place? The best guess here is that Skype is under Microsoft's umbrella of software. Microsoft allows users of its products (such as Xbox, Office, Windows, and Skype) to use one universal login. With access to Skype credentials, an attacker can access everything in a Microsoft user's library. This allows for a plethora of possibilities, from banking fraud to identity theft to even more phishing attacks.

COVID-19 themed attacks targeted the World Health Organization (WHO) is another example of how phishing can cause havoc to cybersecurity.

The World Health Organization (WHO) has seen a massive increase in cyberattacks from all fronts including phishing attacks. Just recently, the WHO reported that a cyberattack resulted in the leaking of credentials of employees.

This knowledge was made known publicly via the WHO's official website in a press release. The release said this specifically about the nature of the leaked credentials:

This week, some 450 active WHO email addresses and passwords were leaked online along with thousands belonging to others working on the novel coronavirus response. The leaked credentials did not put WHO systems at risk because the data was not recent. However, the attack did impact an older extranet system, used by current and retired staff as well as partners. WHO is now migrating affected systems to a more secure authentication system.

This week, some 450 active WHO email addresses and passwords were leaked online along with thousands belonging to others working on the novel coronavirus response. The leaked credentials did not put WHO systems at risk because the data was not recent. However, the attack did impact an older extranet system, used by current and retired staff as well as partners. WHO is now migrating affected systems to a more secure authentication system.

In the same press release, the WHO confirmed that it has seen a "fivefold increase" in cybersecurity attacks. Experts believe that a variety of factors contribute to this. Speaking with SC Magazine, Lucy Security CEO Colin Bastable gave his opinion on the reason for the increase.

He pinpointed two primary driving factors, the first being cybercriminals looking for any avenue to gain more ways to social engineer. These credentials allow for faking of emails and advertisements used in phishing scams. Bastable's second reason was political. According to the Lucy Security CEO, Bill Gates' affiliation with the WHO is possibly inspiring politically motivated hacking:

> The leaks may also be tied to political hostility to the Gates Foundation's work on vaccinations and its participation in an October 2019 pandemic wargaming session, Event 201... 'leak' may be... designed to capitalize on the WHO's woes and [Microsoft founder Bill] Gates's drive to promote his Foundation's vaccines combined with tech-based lockdown 'passports.'

The World Health Organization is likely only going to see further cyberattacks increasing in an exponential rate, at least until the crisis is over.

As we stand together during this COVID-19 pandemic, the world's security teams are actively working together to bring issues into the light so we can combat cybersecurity threats together. The Tech Hero team is here to support you.

Client Spotlight

easterseals
all abilities. limitless possibilities.

Easterseals celebrated their centennial anniversary last year, originally known as the National Society for Crippled Children. This iconic organization has a rich history in the business of giving. As America's largest nonprofit healthcare organization, Easterseals is committed to the comprehensive health and wellness of the more than 1.4 million people it serves each year. Easterseals is prepared to respond to the needs of the one in four Americans living with disability today with outcomes-based services for all disabilities throughout the lifespan.