August 2020

A quarterly newsletter of the Diocese of Trenton Risk Management Program

Diocese of Trenton Risk Management Quarterly

Parishes, Schools, Cemeteries & Catholic Institutions

Fall Edition

Protecting God's Children:

Safe Virtual Environments

Source: Virtus. This is an abridged version.

Never has the concept of "virtual boundaries" been more important than today as more people sign on to various virtual platforms to connect with others. We need to learn how to define boundaries clearly to assure that our online behavior is appropriate.

We must adapt our teaching, preaching and communicating in order to provide children with a safe virtual environment. Regardless of your role or position in the life of a child, this article will provide you with appropriate boundaries and best practices for online interactions with youth.

Our lives are made up of a series of relationships. These include relationships between family members, colleagues, peers, acquaintances, mentors, friends and others. Every healthy relationship requires a series of boundaries which enable us to comfortably and effectively communicate. Boundaries vary depending on the relationship and the context of the encounter.

Challenges of boundaries in online settings

Boundaries in online, virtual settings are new to many users and can be challenging to set and maintain. The virtual platform, application (app) or online setting becomes a "location" that is often outside of the sight and hearing of others. Serious risks can occur when adults fail to maintain proper boundaries. For young people, the online environment usually is social and for entertainment. In the last months, children and teens have had to adapt to daily classrooms that are virtual. It is not unusual for youth to misunderstand the nature of relationships shared online. Interacting via technology allows for personal thoughts, emotional content and private feelings to be shared more readily than "in person."

Technology also allows for one-on-one conversations which may be outside of the supervision of other adults. It may create a more relaxed context where well-meaning adults forget to maintain a professional persona. It can also increase opportunities for the undetectability of people who don't have the best intentions.

The majority of adults serving youth will not intentionally abuse the nature of online interactions. Some may make honest mistakes due to a lack of experience in using technology as a teaching or ministry tool. All of us have a greater responsibility to ensure that our own behavior is appropriate. This allows us to accomplish the goals of specific online interactions and to assure that we don't unintentionally condition a child to accept someone else's inappropriate online behavior. Regardless of your role in the life of a child, the main goals of your online and live interaction with youth are the same: provide children with what they need and keep them safe while doing it.

Best practices for caring adults who are utilizing technology as a means of communication

For those who are working with, or ministering to, youth through technology—whether temporarily or in long-term situations—there are specific rules and best practices to follow regarding social media, online interaction and the Internet. Make sure that you are aware of your Diocesan, Parish or school policies.*

Following are additional best practices on how to safely interact with minors in your care while appropriately meeting, chatting, educating, visiting and ministering to them via the Internet.

continued on page 2

Safe Virtual Environments, continued from page 1

Best practices for all youth-serving adults:

- **Utilize technology (devices, applications and platforms) sanctioned by the organization.** Use only those programs, platforms and applications that have been provided by your Parish or school. If you find a helpful program, share it with your supervisor for approval before using it with young people.
- **Keep personal social media accounts private.** Adults working or volunteering with youth should not use their personal emails, phone numbers or social media accounts to communicate with minors. If the organization does not have its own official account for you to use, work with supervisors to create one that allows you to block your identifying information. Make sure that all supervisors have access to the accounts you are using for meetings with youth.
- **Avoid "friending" or communicating with minors using personal accounts or private messages.** Under no circumstances should a caring adult be utilizing a personal account to send a "friend" request to a minor who is in their care, or who is known to them because of work or ministry.
- **Meet with minors in online groups, and never one to one.** Virtual meetings can include other students or parents to maintain transparency. Other adults in your organization should also be included when possible and/or necessary for proper oversight.
- **Maintain appropriate communication with both minors and other adults.** Anything sent to an individual minor should also be copied to his or her parent or guardian. Keep language professional and formal just as you would "in person."
- **Communicate with youth during appropriate timeframes.** While it is understandable that sometimes normal operating schedules can be interrupted, it is imperative that proper boundaries are observed when communicating specifically with minors. Your organizations should establish all scheduled time for meetings.
- **Be mindful of what students will view and hear from your own surroundings during online meetings/classes.** Educate youth on creating an appropriate background for online meetings. Tell them to check what is behind them on walls. Have them consider how certain spaces such as sitting on a bed may be inappropriate. Remind them to inform their family that they will be having a virtual meeting so that those in the area are properly attired and are cautious with conversations. Coach youth on appropriate attire for your virtual meeting. Be sure to take the same care when preparing your environment.

Accept the increased responsibility to intervene if you see or suspect inappropriate content or evidence of abuse

Youth-serving adults are wonderful for many reasons—one of which is because they are vigilant about protection when children are in school or activities. Sometimes this means communicating to child protective services when there are signs or suspicions of child abuse and neglect.

When kids are not in school or in public activities during times of stress, they can be at greater risk because they don't have that additional contact with people who are there to help them. Red flags of abuse aren't as obvious when someone is behind the technology screen. When interacting with youth online, caring adults must respond appropriately to anything said or observed that may put youth in harm's way.

Helpful reminders:

- **If you see something inappropriate or illegal, it's essential to communicate it to the right person or place.** As with in-person contacts, Pastors, Directors of Religious Education, School Administrators and all Educators are mandated reporters of child abuse and neglect. If after virtual contact with a minor, it appears that this child is a victim, mandated reporters must call the Division of Children and Family (1-877-652-2873). If there are questions about when and what to report, go to **www.nj.gov/dcf/reporting/how/** or contact the Office of Child Protection. You can reach Joe Cahill or Joe Bianchi on the Diocesan hotline (1-888-296-2965) or through **abuseline@dioceseoftrenton.org**. Information should also be reported to **report.cybertip.org** when abuse occurs through a website
- Your online behavior matters, even if no one is "watching." Build a positive and professional online reputation so you are teaching minors what they should expect from safe adults online.
- Sometimes coping assistance is needed when we are anxious, sad, stressed or overwhelmed during times of uncertainty. This happens with youth, too. A professional's help can be enlisted. Take a moment to breathe and evaluate! If an adult or youth in your life needs more help than you can (or should) provide, consider the resource of online counseling or therapy, which is an alternative for people who are unable to go to an actual office for help. Speak with the parent of the minor and consult with your supervisor.

Let us partner together on how to best serve youth during times when we are limited to virtual contact. Becoming more aware of the risks, behaving transparently, and intervening when others' behavior seems concerning helps to protect children and those who genuinely care for their welfare.

*Trenton Diocesan policy on the proper use of technology can be found at **dioceseoftrenton.org/policies-forms** under the heading of Social Media Policy - Office of Communications. ■

The Disruptions of COVID-19: Self-Care and the Diocesan Employee Assistance Program

As we enter Week #23 of COVID-19 nationwide shutdowns, we may be taking stock of the several months behind us and looking with some apprehension to the months ahead.

There is no doubt that along with the viral *infection*, we have experienced a *disruption* of our personal and work lives: face masks, quarantines, curfews, remote work, technology overhauls, supply shortages, and social distancing. Change has been our constant and has touched nearly every aspect of our lives. The stresses of continual and rapid change, isolation, learning new ways of working and living, financial strains and general uncertainty have caused, for many, turmoil in overall physical, emotional and mental well-being.

The Diocese understands the pressures you may be facing during this pandemic and wishes to remind everyone of the 24/7 availability of the employee assistance program benefit designed to offer assistance with personal and work-life issues for all of our staff and your dependents. We recognize that life has become more complicated than ever. Often complicating the matter is the inability to find the right person or resource that can help in the time that it's needed the most.

*EmployeeConnect Plus*sm through Lincoln Financial is just a phone call away, is 100% free and is 100% confidential. There are no insurance claim forms, deductibles or wait time. Help is available 24/7 simply by calling the toll-free number.

*EmployeeConnect Plus*sm services include:

- **Confidential counseling.** This service will connect you to a trained clinician who will help locate in-person counseling and other resources to assist with grief, loss, substance abuse, job pressures, relationship conflicts, stress and anxiety.
- **Work-life solutions.** Work-life specialists can provide qualified referrals and customized information for such things as child and elder care, moving and relocation, college planning, pet care or home repair.
- **Financial information and resources.** CPAs and financial planners are available to assist with a variety of financial issues such as debt management, tax questions, retirement planning, estate planning, college savings and real estate questions.
- **Legal support and resources.** You can speak with an attorney by phone to locate the right type of qualified local attorney for a free 30-minute consultation and a 25% reduction in customary legal fees. Employees or dependents can get assistance with family law, bankruptcy, landlord/tenant issues, real estate transactions civil and criminal actions, etc.

This service is completely FREE. Use of the service is completely CONFIDENTIAL. The service is AVAILABLE 24/7.

Informational Benefits handouts are also available from the Employee Benefits Office at the Chancery. Contact Erica Armitage, earmit@dioceseoftrenton.org or 609-403-7219. ■

Update on the Sensor Program

Over the past 3 years, the Diocese has been working with HSB on a sensor program designed to help mitigate loss from frozen pipes and water damage. To date, 20 properties currently have the sensor program installed. The Diocese is looking to add 40 more properties by the end of the year.

Why a Sensor Program?

Recently, a parish in Mercer County filed a water damage claim of more than $70,000. The damage resulted from a failed water supply line to a refrigerator icemaker. The rectory was unoccupied at the time so the water ran for 20 to 28 hours. The water spread through the first floor kitchen, dining room, hallway, bathroom, foyer, and cascaded down to the basement, causing damage to flooring, walls, and cabinetry. There were no water sensors installed in this location. Had the water sensors been installed, this claim may have been significantly less, possibly as little as $5,000, not to mention the amount of time needed to make the repairs which would have also been significantly less.

Positive Results

There have been over 20 confirmed incidents where the sensors saved the Diocese from a significant claim. In one location, a solenoid valve failed on a heating system in an unoccupied religious school building, causing water to spray into a classroom. A facility manager received a text indicating there was high humidity in that space, prompting him to check on the building. He was able turn off the water and contain the leak in time before significant damage occurred.

The damage was limited to just 1,000 square feet of the one classroom instead of possibly 20,000 square feet of the entire first floor of the school. The water would have continued to spray over the weekend and would not have been discovered until Monday if it had not been for that alert.

Now is the Time

Many buildings are unoccupied right now because of the current pandemic. As evidenced from the parish in Mercer County, water damage can happen any time of the year. And with so many buildings unoccupied, a small leak can go undetected for a long time. The longer it goes undetected, the greater the damage. And while it is summer outside, fall and winter are on the horizon. With the cold weather comes the risk of frozen pipes. In addition to detecting water, the sensors can detect when temperatures become critically low - low enough to freeze pipes. Now is the time to prepare buildings and help protect them from significant water damage caused from leaks or frozen pipes.

For more information about participating in the program in the future, please contact Joseph Cahill, Director Risk Management at (609) 403-7189 or jcahill@DioceseofTrenton.org. ■

Items of Importance

Wireless Microphones – Important Information

Is the wireless audio broadcast equipment in your church and school compliant with new FCC regulations?

Reallocation of wireless broadcast frequencies started in 2017 with a significant portion of the 600 MHz frequencies being repurposed for additional TV band spectrum. The currently available spectrum for wireless microphones has decreased as a result of the spectrum auction, which was completed on April 13, 2017. Specifically, most (but not all) of the spectrum on TV channels 38-51 (614-698 MHz) has been repurposed and will no longer be available for wireless microphone use.

Wireless microphones that operate in the 600 MHz service band (the 617-652 MHz and 663-698 MHz frequencies) will be required to cease operation no later than July 31, 2020 and may be required to cease operation sooner if they could cause interference to new wireless licenses for TV broadcast services. See FCC 15-140. Spectrum will continue to be available for wireless microphone use on TV channels 2-36 (TV band frequencies that fall below 608 MHz), on portions of the 600 MHz guard band (the 614-616 MHz frequencies) and the 600 MHz duplex gap (the 653-663 MHz frequencies), and in various other spectrum bands outside of the TV bands. See FCC 15-100, FCC 15-99.

Check with your sound system vendor to determine if your current system will be out of compliance on July 31st. Fines for operating non-compliant wireless systems can be significant.

Property/Casualty Insurance Premiums

Property/Casualty insurance invoices for the 2021 fiscal year were distributed during July. On average, premiums increased 6.29%. A breakdown of premium changes is listed below.

Premium decrease	19%
No increase to 5% increase	40%
5.1% increase to 10% increase	24%
10.1% increase or more	18%

The renewal of most of our excess insurance policies on November 1st will be challenging. COVID-19 has become a significant factor in the renewal of all property, liability and workers compensation programs due to the uncertainty of future losses.

The property market has been hard for the last year, with average premium increases topping 24% due to concerns related to catastrophic weather events. COVID -19 has a potential impact on property policies as business interruption coverage is contained in property policies. Many policies specifically excluded viruses, pandemics and events that don't relate to physical property damage; however, many states are attempting to re-write policy provisions retroactively. The courts will ultimately decide the coverage issues, but early indications are not favorable to the insurance carriers which will seek large premium increases in combination with coverage reductions at the next renewals.

Our Cyber Carriers have already indicated that our $10 million in coverage will probably be reduced to $5 million with a 25% to 50% or more premium increase. Property increases as of July 2020 are pushing the 25% to 40% range with larger increases expected for renewals in October through December. The expected increases will dramatically affect parish premiums next July.

As a primarily self-insured entity, we can minimize premium increases for the 2022 fiscal year by making the extra effort to minimize losses across all lines of coverage – property, general liability, cyber, employment practices and, most of all, workers compensation. Many claims related to property, cyber and workers compensation are avoidable losses. The deployment of the HSB Environmental Sensors can significantly reduce property damage claims. The list of avoided losses at properties utilizing the system continues to grow, attesting to its effectiveness as a valid loss control measure.

The deployment of CarbonBlack CB Defense and BlueVoyant's active monitoring and management service is another effective tool for loss minimization. Workers compensation losses are truly employee safety issues. More needs to be done to effectively protect our work associates through training, better building and property maintenance and the elimination of workplace hazards.

PosterGuard – Employee Workplace Postings

PosterGuard has resumed shipment of poster updates as of June 2020. Other than State-issued temporary posting for COVID-19, social distancing and several guidance documents not applicable to employees of the Diocese, there have been no major updates released.

COVID-19 related information is available at **https://www.nj.gov/labor/employer-services/business/covid.shtml and https://covid19.nj.gov/**

A listing of employer required postings is available at **https://www.nj.gov/labor/lwdhome/content/employerpacketforms.html**

NEW Legislation - Pending

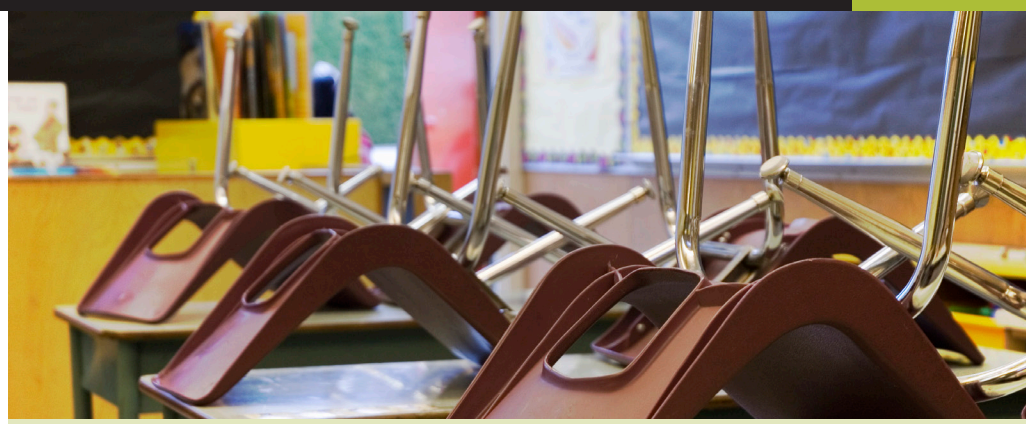
New legislation was proposed by the Governor in February 2020 to amend New Jersey's anti-workplace harassment laws for public and private employees.

- The legislation will establish standards for hostile work environment claims including the stipulation that **a single act** can constitute the basis for a claim of a hostile work environment.
- Employers must adopt a **written anti-discrimination and harassment policy**, including sexual harassment.
- **Mandatory training**: employers will be required to provide employees with interactive workplace training on unlawful discrimination and harassment, including sexual harassment.
- **Mandatory reporting**: Employers with more than 50 employees will be required to collect and annually report on all complaints received, including sexual harassment.
- **Extends statute of limitation** for cases brought under LAD (Law Against Discrimination) from 2 years to 3 years and the statute of limitation for filing a complaint with the DCR (Division on Civil Rights) from 180 days to 1 year.
- **Broadens the definition for employee** to include domestic workers and unpaid interns to employees protected by LAD.

NEW Legislation – Signed

New legislation was signed by the Governor, effective March 25, 2020, requiring that all employees receive a maximum of 40 hours of paid sick leave per year. Full-time and part-time employees are eligible with few exceptions. The revision in the legislation includes sick leave related to a state emergency declared by the governor or when necessary as indicated by the Commissioner of Health or other public health authority. ■

Vigilance: Protection of Unoccupied Buildings



Over the past 5 months, many of our parish and school buildings had to be left unoccupied. As we continue to await what the future may bring, please take steps now to protect your unoccupied buildings from theft, vandalism, and property damage so that we may all soon return to our safe and cared-for places of worship, work and school.

A recent example of property damage during a shutdown was at a temporarily-unoccupied parish owned building. A water line to a refrigerator ice maker leaked, flooding a significant portion of the first floor and causing additional damage in the basement. The flooding lasted for more than 20 hours before it was discovered. If water sensors had been deployed, the leak would have been detected within minutes and the building owner notified.

Unoccupied Building Risks

Buildings that are unoccupied are subject to greater risk from certain types of perils. An interruption of utility service, vandalism, or even a faulty furnace can cause significant damage if it goes undetected. Implementing loss control measures can help avoid damages and costly property and liability claims. Inspecting and ongoing monitoring of these properties is the key to protection. The HSB sensor program is performing tremendously well and we encourage the continued deployment of Environmental Sensors products and services through our rollout. Contact Joe Cahill to schedule an installation: jcahill@DioceseofTrenton.org

Before Shutting Down

Before temporarily shutting down for any time period that buildings may be unoccupied, take a tour of your building and grounds. Are drains unobstructed? Are sump pumps operational? Are all windows and doors in good repair and equipped with functioning locks? Have the fire and smoke detector systems been tested? Are you able to account for all keys to the building? Remember to remove all perishables from the refrigerator, unplug the unit and leave the door open to promote air circulation. For more suggestions, please download our checklist: **www.dotinsurance.org/facility-checklist**

During the Shutdown

Be sure a plan is in place to maintain the grounds on a regular basis, including mowing lawns, trimming shrubbery and pruning trees. Plan on-the-ground inspections at least weekly. Always visit your facility after heavy storms or during extended periods of high humidity. Look out for the following:

- Check entrances to ensure they are secured
- Check windowpanes for breakage and make sure locks are intact
- Look for signs of vandalism, graffiti, or attempted break-ins
- Inspect for evidence of pest intrusion or insect damage
- Remove any debris from the grounds
- Check interior for any signs of leaks, condensation or water accumulation
- Test and, if necessary, change exterior light bulbs

In addition to the on-the-ground inspections, you may want to drive around the property on a regular basis. At the very least, inform local police that the building will be unoccupied and request that they routinely drive by the building, especially in the evening.

Preventing Vandalism

Doors and windows need to be locked and in good repair. Greenery should be removed so there is a clear view of the windows and doors. Ensure that adequate exterior lighting is available and functioning. This will not only help deter criminals but will also help personnel establish a quick visual assessment in the event of a broken window or other vandalism. Keep shades/blinds up so police or neighbors can see individuals inside the building during off hours. Broken windows or doors need to be quickly repaired or boarded up to deter vandalism and trespassing.

Mold Prevention

When buildings are unoccupied, one of the biggest threats is mold growth. The risk for mold growth is especially high during extended periods of hot, humid weather, when it can begin to grow on wet walls, carpets or flooring within 24 to 48 hours. The HSB Environmental Sensors that monitor temperature and humidity will alert the property owner when conditions exist that promote the growth of mold. The algorithm developed and beta tested almost a year ago has been very effective in alerting property owners when conditions are ripe for mold growth so that corrective action can be taken. In many cases, its as simple as changing the temperature setting of the thermostat or improving air circulation. Please take these steps to prevent mold:

- Reduce indoor humidity by keeping moisture below 60% relative humidity. Between 30 and 50% is ideal. Control humidity levels and dampness by using air conditioners and de-humidifiers.
- Provide adequate ventilation. Keep interior doors open and cross-ventilate when possible.
- Contact Scot Pirozzi or Joe Cahill for assistance. Act fast to clean and remediate if you suspect or see any mold growth. ■

Vigilance through Volatility: Weathering the Storm

The National Hurricane Center predicts a 60% chance of an above-normal season for the Atlantic in 2020. The season is already off to a strong start with Tropical Storm Isaias.

The effects of even a small tropical storm can leave tornadic, strong wind and flood damage hundreds of miles inland from the coast. Properties not located in an official flood zone are most often just as susceptible to damages.

Although the Atlantic hurricane season runs from June 1 through November 30, the peak is usually August to October. Preparation and planning is needed NOW. Secretary of Commerce Wilbur Ross advises, "As Americans focus their attention on a safe and healthy reopening of our country, it remains critically important that we also remember to make the necessary preparations for the upcoming hurricane season."

Now is the time for 3 R's: Review, Reassess and Readjust your business preparedness and disaster response plan. Keep it simple: use the guidance below to outline your plan and preparations, as well are your response and actions during the aftermath.

Your plan should include:

- Up-to-date contact information and communication procedures/protocols/ notifications
  - Employees and staff
  - Local emergency agencies/remediation vendors
  - Diocesan Office of Risk Management/ Chancery contacts
  - Claim reporting contacts (**dotinsurance.org/coverage/manual**)
  - Designated Emergency Response Team members
- A list of activities to be performed in advance of a storm:
  - Communication on website/postings on buildings
  - Shutdown of utilities (electrical, water, gas)
  - Identify and order emergency supplies, such as plywood, sandbags, mops, brooms, tarpaulins, waterproof containers, etc.
  - Identify key equipment, supplies, and vital records that need to be relocated, covered and raised off the floor and moved away from windows and doors.
  - Test equipment such as backup power, generators, sump pumps, etc.
  - Ensure fuel-fired equipment tanks are full.

Outside of the Building

- Check the windows/window sills for rot, open areas and opportunities to repair, enclose or protect from wind and water.
- Check the roof covering, flashing and roof drains. Make all necessary repairs securing any loose items and clean drains for best chance of water diversion.
- Check the premises for items that need to be removed to prevent airborne destruction (benches, unreinforced parapets, decorative facades, unsecured mechanical equipment, chairs, loose tree limbs, statutes, etc.)
- Close and latch exterior doors and windows, board and brace large windows and doors.
- Deploy flood barricades and other protective measures when the National Weather Service issues a local Storm Watch but no later than immediately after an upgrade to a Storm Warning and at least 24 hours in advance of anticipated landfall. Early deployment is the best policy.

Inside of the Building

- Relocate furniture and equipment away from windows and doors.
- Raise or relocate equipment and furniture.
- Tarp and cover items.
- Move paper records to waterproof bins to relocate off premises or elevated levels.

After the storm

- Take photos and video of the property, including any visible damage
- Report all damage to the Diocesan Office of Risk Management. Joe Cahill, cell: 732-284-1600, or Joe Bianchi, cell: 732-267-0381 for assistance.
- Assume that all downed power lines are fully energized under all circumstances and avoid them. Before utilities are returned to service, check for gas leaks, look for electrical system damage, and check for sewage and water line damage.
- Wear proper personal protective equipment, such as steel-toed work boots, thick gloves, eye protection, dust masks and other safety equipment.
- Should you need to shut down a fire sprinkler system during restoration, **follow the proper impairment procedures and notify the alarm company if alarm systems are placed in standby mode.** Follow proper permit procedure for any hot work that you may need to perform. Hot work includes the use of any flame or heat-producing device used for welding, brazing, grinding and soldering.
- If safe, make emergency repairs and commence with salvage procedures to try to keep any additional damage from occurring.
- Clean debris from roofs and property, if safe to do so.
- Remain aware - stay tuned to local radio for information.
- Review emergency plan execution post-mortem to revise for the future. ■

COVID-19 and the Phishing Evolution

Edited from an article by Courtney Maugé, Willis Towers Watson

Reports of phishing attacks have tripled since the concerns about COVID-19 became widespread. According to Willis Towers Watson's 2019 Reported Claims Data, 63% of cyber incidents were caused directly by human errors. Understanding phishing scams is more critical than ever.

COVID-19 Phishing Scams

Phishing campaigns are an effective method for cyber criminals to access protected networks because they feed upon human psychology and trust and, in times of crisis, prey upon the fears of millions. In addition, the sudden move to a remote working environment may have contributed to increased distractions and the decreased likelihood that remote workers would authenticate the validity of emails with colleagues. Thus, COVID-19 seems to have opened an entirely new playground for cyber criminals. Studies show that in the first 100 days of COVID-19, there was a 30% increase in impersonation fraud. By mid-April, reports showed cyber criminals sent 1.5 million pandemic-related malicious emails per day. Many experts declared the large volume of COVID-19 related scams the largest coalescing of cyber attacks to exploit a single theme.

The U.S. Department of Homeland Security warns companies to remain vigilent about emails containing coronavirus in the subject line, COVID-19 related website links, and COVID-19 related emails containing file attachments. In early April, one campaign sent emails promising access to important information about cases of COVID-19 in the receiver's local area. The emails evaded top email malware-detection software, resulting in the theft of users' Microsoft log-in credentials.

A later analysis revealed cyber criminals were targeting individuals with emails that appeared to come from the U.S. Department of Labor regarding changes to the Family Medical Leave Act, containing attachments deploying Trickbot Malware. Further studies uncovered creative campaigns related to bonus reports, COVID-19 disaster relief, pandemic food distribution, office shut downs, FedEx packages, quarantine protocols, and changes to insurance plans. Campaigns that appear to come from trusted government sources such as the White House, the CDC, and the World Health Organization continue to trend.

COVID-19 related phishing emails can be hard for an employee to spot. According to one study, most of the COVID-19 related phishing campaigns appeared to come from IP addresses located within the U.S. While it is possible that the IP addresses could have been manipulated, it points to a more concerning reality: when phishing campaigns stem from the same geographic region, it is easier to mimic the culture and language of that region. In other words, phishing campaigns are more likely to sound, look and feel like they come from legitimate sources. Also, these emails may be more prone to bypass firewalls, meant to only block foreign IP addresses. Additionally, the same study found that many of the emails contained company logos, trademarks and copyrights, making them look almost identical to legitimate company emails.

Finally, amid growing cyber risk concerns, an analysis of Google search results during the core months of the U.S. pandemic revealed an increased interest in searches pertaining to hacking, scamming and other forms of cybercrimes. Breakout search terms such as "hacking course" and "ethical hacking course" reached record highs.

COVID-19 has only exacerbated cyber criminals' ability and desire to take advantage of the human element of cyber risk. As the fallout lingers, companies must remain vigilant and continue to inform employees of the increased social engineering risks tied to COVID-19.

What to Expect as the Economy Reopens

Threat actors continue to become more sophisticated in their tactics and will continue to exploit trends and global events to conduct phishing campaigns. While COVID-19 email subject lines will inevitably decrease as lockdowns are lifted, companies should operate under the assumption that social engineering attacks will continue and should be prepared to respond appropriately. Managers should implement lessons learned from COVID-19 into routine employee trainings. Employee understanding of how to spot and report email scams is critical to a company's success in preventing cybercrime. In addition, business continuity plans, as well as adequate crime and cyber insurance, will be key in the event of a successful social engineering attack.

Tools to Combat Cyber Crime

The Diocese of Trenton has deployed CarbonBlack CB Defense in conjunction with the active monitoring and mitigation services of BlueVoyant to combat malware, ransomware, and attacks on networks for the last several years, to great effect.

Over the last two years, multiple cyber events have affected parishes and schools that had not fully deployed CB Defense endpoints on every computer in their networks. With the realities of working from home, remote access is a significant concern. The Computer Services Department of the Diocese is always available to review and advise on all network security measures and secure remote access. Contact Anthony DeLorenzo at **ADelor@DioceseofTrenton.org** ■

Roman Catholic Diocese of Trenton
Department of Administrative Services
701 Lawrenceville Road
Trenton, NJ 08638

FIRST CLASS MAIL
US POSTAGE
PAID
MAILED FROM ZIP CODE 07006
PERMIT NO. 881

Fall Edition

Diocese of Trenton Risk Management Quarterly

Parishes, Schools, Cemeteries & Catholic Institutions

Inside this Issue:

Risk Management Key Contacts

Willis Towers Watson Team
Willis Towers Watson Southeast
Concourse Corp. Center 5, 18th Fl.
Atlanta, GA 30328

Jen Adams, Assistant VP
Tel: 404-302-3841
Jen.Adams@willistowerswatson.com

Mike Farrand, Sr. Principal
Tel: 610-715-1951
Mike.Farrand@willistowerswatson.com

Alex Lok, Sr. Client Specialist
Tel: 404-302-3824
Alex.Lok@willistowerswatson.com

Certificates of Insurance
For our online form, go to:
dotinsurance.org/forms/certs

Claim Reporting
PMA Management Corp.
PMA Corporate Processing Center
Tel: 800-482-9826; Fax: 856-727-3186

Auto Insurance Cards
Porter & Curtis, LLC
Tel: 484-445-7174
Email: trenton@aeti-inc.com

For our online form, go to:
dotinsurance.org/forms/auto-forms

Diocese of Trenton
Chancery
701 Lawrenceville Rd.
Trenton, NJ 08638
Main Tel: 609-406-7400

Joseph Bianchi, Chief Administrative Officer
Tel: 609-403-7208
Fax: 609-406-7413
jbianc@dioceseoftrenton.org

Joseph Cahill, Director of Risk Management
Tel: 609-403-7189
Fax: 609-403-7215
jcahill@dioceseoftrenton.org

Scot Pirozzi, Director, Department of Construction and Property
Tel: 609-403-7195
Fax: 609-406-7412
spiroz@dioceseoftrenton.org

www.dotinsurance.org