Diocese of Manchester Cyber Security Best Practices

The following is a list of best practices to combat typical scams and security threats. Failure to follow these rules can have significant negative financial and other impact to your parish, school, organization, or the diocese, can take large amounts of time and cost to correct, and can put our network at great risk!

1) **SCREEN FOR COMMON EMAIL OR TEXT SCAMS**:

    a. **Match the actual email address or telephone number** of the sender to the name of the person who is requesting something from you.

    b. **Read the email or text for unusual grammar or sentence structure**. Be on the alert for any email asking for funds, gifts, or confidential information such as bank account numbers. Some common scams get you to reply with questions "Are you in?" "Can you talk now?" and similar comments to engage you in further email exchanges. Once you have replied, they will try to convince you that they are who they say they are and get you to perform some kind of transaction. Some request wire transfers, gift cards, and changes to an employee's payroll direct deposit.

2) **DO NOT RESPOND TO SUSPICIOUS EMAILS OR TEXTS**: If an email or text requests funds, cash equivalents (gift cards, etc.), or sensitive information, and this is an unusual request, then it is likely a scam. Do not respond. Do not forward the email unless you wish to alert others of the potential scam. In most cases, the best option is to delete the email and report it as a scam to your supervisor.

3) **CONFIRM VERBALLY WITH SENDER BY PHONE:** If the sender claims to be the pastor or other employee of authority and you think there is a possibility of legitimacy to the email, then, prior to responding to the email, contact the sender by phone.

4) **DO NOT CLICK ON ANY LINKS IN AN EMAIL OR TEXT** unless you know that the email is from a trusted source, and you are expecting it. If you have any doubt, do not click on the link before calling the sender to make sure it is legitimate.

5) **DO NOT DOWNLOAD OR OPEN ANY ATTACHMENT IN AN EMAIL OR TEXT** unless you know that it is from a trusted source, and you are expecting it. If you have any doubt, do not download or open the before calling the sender to make sure it is legitimate.

6) **NEVER ENTER YOUR PASSWORD** except:

    a. When logging into your computer

b. When accessing your email via OUTLOOK, your phone app, or a browser, make sure the app is one that you installed. On a browser, make sure it is the correct URL (e.g., gmail.com, Microsoft.com, etc.).

Scammers can make a site look legitimate to try to obtain your password. This has happened with email, banks, PayPal, eBay, credit card, and other sites. Always check the URL to make sure it is really the site that you think it is.

7) **NEVER PROVIDE YOUR PASSWORD TO ANYONE**. You should not give your password to anyone either via email, on the phone, on a website, or verbally unless it is a trusted and known technology person helping you with a problem. Legitimate help desks will NEVER ask for your password – do not give it to them. Do not leave your password on or in your unlocked desk or anywhere it can be easily seen (like on a sticky note).

8) **NEVER PROVIDE ACCESS TO YOUR COMPUTER TO ANY OUTSIDE COMPANY**. A popular scam is to provide a popup on your computer from a website that you are visiting that indicates there is a problem on your computer and to call an 800 number and talk with a Microsoft support agent. There are variations of this scam, but they tend to be similar. The scammer will download software to your computer that allows them to access your data and passwords. There have also been instances where the software they planted has infected an entire network, and they demand a ransom to allow you to access your own data. Never call an 800 number for assistance with your computer. The only people you should be talking with about accessing your computer are a trusted and known technology person.

9) **NEVER SEND MONEY, GIFT CARDS,** or respond to **PURCHASE ANYTHING** for anyone requesting these via email. In all cases, these have proven to be scams! If you think it is legitimate (and it probably isn't), then CALL the person first.

10) **BE CAREFUL WHEN CREATING AND PARTICIPATING IN CONFERENCE CALLS** and using apps such as Zoom and GoToMeeting. The FBI has warned about potential vulnerabilities in the app, mainly that a meeting can be "Zoombombed" – joined by someone who wasn't invited or an inappropriate video added. Be sure to configure meetings so that only the intended guests can join. Do not post screenshots of meetings in real-time on social media, which lets anyone see your Zoom, GoToMeeting, or Microsoft Teams meeting number and opens your meeting up to uninvited people. **DO NOT RESPOND TO REQUESTS TO CONNECT TO UNKNOWN WEBINARS, ONLINE CONFERENCES/CALLS, OR OTHER COMMUNICATIONS**. These are usually accompanied by an invitation to download a communication tool (like Zoom or GoToMeeting), but in reality, it is a virus that can take over your computer and your network to gain access to your files, banks, credit cards, etc. At times they will demand a ransom to get your files restored (known as ransomware).

11) **ENSURE THAT YOUR IMPORTANT DATA IS BACKED UP** to an offsite location. If they are not stored offsite, they can be lost or rendered unusable in the case of an attack.

12) **PASSWORD PROTECT ALL DEVICES.** If you are accessing our system either for email or via VPN, make sure all your devices (e.g., smart phones) are password protected with phrases that are hard to figure out. Passwords should be a minimum of 8 characters, with both upper and lower case letters, a number, and a special characters. Longer passwords or phrases are best (e.g., “Watchnbcsportsifyoucan!”). Change your password at least every 90 days.

13) **USE UNIQUE PASSWORDS FOR EACH SITE/NETWORK:** If your credentials were stolen from a site/network and you use that same password on multiple sites/networks, all of the data contained on every site is now vulnerable. If you use unique passwords for every site, when one is breached, the data at every other site is still safe.

14) **EACH PERSON SHOULD HAVE UNIQUE LOGIN CREDENTIALS (USERNAME AND PASSWORD)**. Each regular user should have separate credentials to login to a device, even if the device is shared by multiple people; each regular user should have separate credentials for each online account such as e-mail systems, payroll software, and accounting software; guests should use a separate login account dedicated to guests that does not have administrative privileges on the device. Use Delegation features when appropriate to grant access without requiring providing the password when multiple people are utilizing a shared email account.

15) **USE MULTI-FACTOR AUTHORIZATION** wherever available. For example, when logging in from a new device, the system will send a security code to your phone or email before allowing access.

16) **USE BCC:** When you send out an email to a distribution list, send it via blind copies (i.e., bcc). That way, potentially scamming recipients (or one who has been hacked) does not have access to a large list for fraudulent emails.

17) **LET YOUR PARISH, SCHOOL or ORGANIZATION KNOW:** Put announcements in bulletins, newsletters, and periodically remind people from the pulpit or at group meetings that neither the pastor, principal, nor any staff members will ever ask for money, donations, gift cards, etc. via email or text.

18) **CONSIDER A CONTACT FORM ON YOUR WEBSITE:** Rather than include direct email addresses on your parish, school, or organization website, consider a “Contact Us” page that sends an email without displaying email addresses to the site visitor. This makes it harder for the addresses to be impersonated and used in email scams.