CWL Diocesan Communications Communique #3 – March 2018

To: Parish Council Communication's Chairpersons

From: Lynn Jones, Regina Diocesan Communications Chair

Whether you agree or not with the trend towards electronic communication we need to be able to protect ourselves and the messages we are sending and receiving from potential social engineering.

Social Engineering is the art of manipulation, influencing or deceiving you in order to gain control over your computer system. Electronic hacking is no longer the most damaging of security penetrations.

As the Catholic Women's League moves towards more and more online communication please keep in mind the following RED FLAGS when working with emails:

When you are receiving an email FROM someone else please keep the following in mind:

1. I don't recognize the sender's email address as someone **I ordinarily communicate with**.
2. This email was sent from **someone from the CWL** and is **very unusual or out of character**.
3. Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
4. **I don't know the sender personally** and they **were not vouched for** by someone I trust.
5. This is an **unexpected or unusual email** with an **embedded hyperlink** (link to a website) **or an attachment** from someone I haven't communicated with recently.

When you are receiving an email TO where you were cc'd or it was sent to a group:

1. I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
2. I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people with the CWL whose last names start with the same letter, or a whole list of unrelated addresses.

When you are receiving emails with HYPERLINKS embedded in the message:

1. I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
2. I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
3. I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."

When you are receiving an email with an unusual DATE or TIME:

1. Did I receive an email that I normally would get but it was **sent at an unusual time** like 3 a.m.? Did I receive it from someone I know is away and has no access to email?

When you are receiving emails with a suspicious SUBJECT line:

1. Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
2. Is the email message a reply to something **I never sent or requested**?

When you are receiving emails with ATTACHMENTS:

1. The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
2. I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file. Word and Excel are also common file types but they two can have embedded virus's.

When you are receiving emails with suspicious CONTENT:

1. Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
2. Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
3. Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
4. Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
5. Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

Just like you would protect yourself when walking through a parking lot at night or an area of town you are not familiar with, or taking a phone call from someone promising you a lot of money; you need to also protect yourself against harmful emails.