SLIDE 1  Welcome to our Cyber Safety workshop.

While cyber scams are not new, we have recently seen an uptick in cyber scams in P.E.O. Today,

we will review specific cyber scams and how to protect yourself from these scams not only in

P.E.O. but in your home and work life, too.   This will be a lot of information so please note that

on page \_\_\_\_\_\_\_ of your delegate packet, there is a recap for you to share with your chapter

sisters when you have your Report of State Convention.  Please make a copy to give to each

sister.

SLIDE 2 Let’s focus on Phishing. What is Phishing?

It is a type of cyber attack where unwelcomed messages, either by email, phone or text, are

sent pretending to be a trusted person.  The attacker is attempting to steal confidential

information such as login credentials, card details or passwords.   They can request money or

gift cards to sources we hold dear and use them for themselves.   These attackers are very good

at their jobs.   They are able to make the requests look very real.  We need to be vigilant in

looking for poor spelling, grammar mistakes, incomplete sentence structure, etc. as most

phishing is generated outside of the USA and Canada. These phishing attacks will also

come  unexpectedly, with usually an urgency to them.

SLIDE 3 There are many kinds of phishing. Let’s review some of them. They may not all apply to

you or to P.E.O. but are worthy of discussion.

READ SLIDE

SLIDE 4  READ SLIDE

As you can see, we must be ever vigilant both in our professional and personal lives.   We live in

a P.E.O. world and in such, we are trustworthy.   Why would anyone ever think to target our

organization, right?   Most of the time, these hackers have no idea who their target is.  They

phish to see if they can get anything out of anyone.   These scams are hurtful and in many

cases, cost individuals in any organization, money.  Yes, even in P.E.O. because a P.E.O. trusts

that the sister who is supposedly asking for something, truly needs it.   Once a sister finds out

that they have been scammed, they are hurt, feel sickened for being sucked into the scheme,

and are embarrassed. It’s natural to feel this way but I am here to tell you that sadly, it happens

all the time.  We have to rise above it and learn how to prevent it from happening again.

SLIDE 5  Now that we are well-versed in all the different kinds of phishing, let’s look at how to

protect ourselves from falling victim to them.

Be suspicious:

●  Of requesting personal data

○  Odd requests are enormous red flags. Legitimate banks or other

companies will never ask for personal credentials via email. You should be

suspicious of emails requesting sensitive information.

●  Be suspicious of spelling and grammatical errors

○  You may get an email from Alabama P.E.O. that contains typos. We will

not deny that. Please forgive us. We are human AND volunteers.   Legitimate

messages from banks, from Facebook, usually do not have major spelling

mistakes or poor grammar.

●  Be suspicious if communication is unexpected or from a company or organization

with whom you do not have a relationship

○  If you do not bank with Wells Fargo and they are emailing you requesting

information, be suspicious.

●  Be suspicious when an email asks you to click on a link

○  Hover your cursor over a link and the web address will appear. Review it

for accuracy, but DO NOT click the link unless it looks legitimate.

●  Be suspicious if the sender’s email address is different than the one in the roster

or website

○  Review the email address carefully. It may just be one letter off from the

sender’s actual email address.

○  It may contain the letters “a i”  which stands for artificial intelligence.

That’s a clear sign

●  Be suspicious if the email has a different URL web address than the one you

typically use

●  And remember, P.E.O. will NEVER ask for donations via email or text!!

SLIDE 6  Let’s see examples that our sisters have received and what others have seen in the

world outside of P.E.O.  Will you be able to find the discrepancies which are signs of a phishing

email or text?  Remember, churches, businesses, community organizations, and schools are also

targeted.

SLIDE 7  Find the errors.   Take a minute to look over.

●  First of all, you can not terminate your P.E.O. membership.   Those are

unfamiliar words.

●  Nancy’s last name is spelled differently.  Two have an “e” and one does not

●  Look at the URL or the link in the box:  International is spelt with a “m” for

“inteMATIONAL.”

●  The URL has “Peosisterhood with numbers”. I’ve never seen that.   Have you?

Exactly.

●  Contains poor grammar and typos such as “To Verify” which is capitalized in the

middle of the sentence.

SLIDE 8  Find the errors:

●  I don’t bank at Ameris Bank.  That is my first sign

●  Email address is not familiar and accounts is spelled incorrectly.  It has only one

“c”.

●  Spelling, grammatical and formatting errors.  “You” is spelled “YCO.”   “Please” is

not capitalized at the beginning of the sentence. The ‘I” in internet is separated

●  A bank would never ask you to verify confidential account information via email.

●  URL is unfamiliar/incorrect.  Again, note the use of numbers in the url

SLIDE 9  Find the errors.  These are text messages.

●  Since I know Perry, I see that his last name is wrong

●  That is not Perry’s number.

●  Grammar and spelling errors:  “siSters”

●  The link has an “a i” in it.   That is for artificial intelligence

●  P.E.O. never gives anything away for free. Well, if you were the first hundreds

to register for CIC in 2021, they did, but not usually. It is noted in our RECORD when it

will happen

●  URL is unfamiliar/incorrect. Note “NOTbankofamerica.”

●  Bank will never ask for confidential information via text.

SLIDE 10 Find the errors.  This is an example of clone phishing.

●  Richard’s email is completely different than what one would expect.   “Mail to:

akua.....”

●  Note the subject matter: URGENT!!! Please, help needed on flight.

●  Dear Sir/Ma. No one addresses Sir/Ma’am as Ma.

●  Email address is different than what a university would use.   .edu versus

@outlook.com

SLIDE 11  This is a screenshot of an email that was sent.  Thank you Patty for allowing us to use

this as an example.  Sisters, please note that this email was not sent to just one sister in Patty’s

chapter.  Many of you received this or a similar email in March from your own supposed

chapter president.  This slide is not inserted to make anyone feel guilty or embarrassed.  It is

here to bring light to how hackers work; how they play on our emotions with powerful

repercussions of self doubt, self worth and pure embarrassment, for allowing this to happen to

us.   So let’s look at this.

●  ”Please confirm by email”

●  I need for you to get gift cards and send them to me”

●  “P.E.O. is giving out gift cards to some cottey students”

●  Reference to the state president

●  “It’s needed ASAP”

●  Signed by Patty and her address is given

This seems, on the surface to be legitimate. It uses terms that we know...Lovingly in PEO and

Cottey students, although we spell Cottey with a capital C.   As busy as we are, almost all of us

would have just said, “Well, if Patty is asking, she must need it”, and go get the cards that she is

requesting.   When you look deeper, you will see that:

 Patty does not live at this address anymore.

 The gmail address is incorrect.  It spells chapter as “chaptar” and what is “presidentA-

Rchapter”?   Please know though, if you are like most of us, you would not have given

this a second look..

It is important to note here that even though this makes us feel like we need to do this

immediately to help, chapter expenses are voted upon AT our meetings so this urgent request

would not have been from Patty.   When in doubt, pick up the phone and call someone to verify

this request before acting upon it.

SLIDE 12  Let’s recap… READ SLIDE

Be on the lookout for notices from your computer about possible phishing.   Some computers

will put a large box across your screen and note that this MAY be phishing so proceed with

caution.  Double check that the email looks right, that the grammar works, that there are no

suspicious links to open. International will send emails with embedded links on occasion as

a convenience for us but will NEVER ask for donations, verifications of membership, or

validation of passwords through a link. Lastly, be on the lookout for incorrect websites.

They are very easy to “misread” so always double check the site before clicking.  If you receive

any suspicious communications, as we talked about earlier, immediately report to your Board

Buddy or any Executive Board officer.

SLIDE 13  We hope that this workshop has presented information that has opened your eyes to

cyber safety. It is always changing and unfortunately, we live in a world where malicious cyber

attacks happen to all of us.   Our sisterhood is no different but we hope that you will have heard

and seen ways to navigate this world and be able to protect ourselves a little better.   The Board

plans to have this workshop posted on our Alabama website for use as a program that can be

shown in your chapter.  Please be sure to reach out to us if you need help with it.  We are

always here for each of you.  Questions?