Keep your club safe!
Cybersecurity tips

WELCOME
Keep your club safe!
Cyber security tips

Presenter Name
Role
Keep your club safe!

Cyber security tips
Hackers will call your phone!

Never give out information over the phone, through email or in person unless the requestor's identity is confirmed.

Instead, call the company back via a published phone number.
If you publish personal information on your website – hackers will probably find it and use it to launch an attack!
Never place personal information including email addresses, rosters, officer lists or district directories on your website.

Never upload (PDF, Excel, Word, etc.) personal member information on your website.

Use contact forms instead of email addresses on your website.

Same rules apply to all social media pages like Facebook.
CYBER SECURITY

• Don't use airport charging stations

• Data access and charging both go through the USB port so hackable

• Use a portable charger instead
• Don't use untrusted wifi networks

• Hackers can impersonate as a known network and then hack your device and steal your information

• Use your phone hotspot instead
Keep your club safe!
Cyber security tips

PHISHING
Phishing

An attempt to obtain sensitive information such as
- Usernames
- Passwords
- Contact lists
- Credit card details
by masquerading as a trustworthy source
Phishing

Often done using
- Email
- Instant messaging
- Texting
- Phone calls
Cyber Security

The biggest security problem online

Phishing accounts for 90 to 95% of security threats
Cyber Security

Phishing victims might be tricked into clicking a link through to a fake webpage.

The aim is persuading the user to enter personal information.
A link can be in the form of a:

- Text link
- Button link
- Image link
Cyber Security

Example of a Netflix Phishing email
It's estimated that an average of 1.4 million phishing websites are created every month.
Some victims are tricked into downloading and installing malware including ransomware and spyware.
Some Definitions

- **Malware** – Any malicious software used to exploit and do harm to a computer, computers or a network.
- **Ransomware** – A malware that holds computer files hostage until ransom paid.
- **Spyware** – A malware that records keystrokes and user activity and sends data to the hacker for exploitation.
- **Social Engineering** - Art of manipulating, influencing, deceiving you to take action not in your or your business' best interest.
You Won!!!

Click Here!

What could go wrong???
Common Phishing techniques include offers of prizes won in fake competitions such as lotteries or contests by retailers offering a 'discount code' or a 'giveaway prize'.
In order to 'win' the prize, the victims are asked to enter their details such as name, date of birth, address and bank details in order to claim. But there's no prize, and all they've done is put their personal details into the hands of hackers.
Phishing attempts claim to be from popular retail, social, government, banks and auction websites – attempting to trick the unsuspecting person.
Spear Phishing

- Key individual(s) or organization are targeted to gain valuable information other than credit card data.
- Targets are researched to make the attack more personalized and increase chances of success.
- Phishers gain trust, then exploit that trust to gain information or access.
Spear Phishing attempts claim to be from friends, coworkers, your HR department, your IT administrator – attempting to lure the unsuspecting person through a false sense of trust.
Actual Spear Phishing Attack on a Kiwanis District

Appeared to come from Governor

Sent to members in the district
How did the hackers do it?
Advanced Search in Google
This search returns any pages that mention "email:" and have "Kiwanis" in the page title.
Attackers now have what they need to launch a Spear Phishing attack!
CYBER SECURITY

Next, the attacker creates an email that resonates with Kiwanians and sends it out, impersonating a Kiwanian.
How can I keep from becoming a victim of Phishing?
Cyber Security

Look for RED FLAGS.

Reg flags warn you to STOP.
Cyber Security

Red Flags of Phishing emails

- Phishing emails cause an emotional response
- They create urgency – act NOW!
- They may carry a threat – something bad will happen if you don't act NOW.
Cyber Security

Red Flags of Phishing emails

- They appear to be from a trusted source
- Make promises too good to be true
- Contain links and direct you to click these links
- Often contain malicious malware attachments
- Often contain typos
RED FLAGS – What to look for

• First of all, STOP and THINK
Anatomy of an email

• "From:" line
Anatomy of an email

- "From:" line
- "To:" line
Cyber Security

Anatomy of an email

- "From:" line
- "To:" line
- "Subject:" line
Anatomy of an email

- "From:" line
- "To:" line
- "Subject:" line
- Date & time sent
Cyber Security

Anatomy of an email

• "From:" line
• "To:" line
• "Subject:" line
• Date & time sent
• Content
Cyber Security

Anatomy of an email

- "From:" line
- "To:" line
- "Subject:" line
- Date & time sent
- Content – Links (text, images and buttons)
Anatomy of an email

- "From:" line
- "To:" line
- "Subject:" line
- Date & time sent
- Content – Links & attachments
RED FLAGS – What to look for

"FROM:" line

• From an unknown address
• If you know the sender but the email is unexpected or out of character
From Costco <manager@eeag.sakura.ne.jp>⭐
Subject Scheduled Home Delivery Problem
To 

Unfortunately the delivery of your order COS-0053845859 was cancelled since the specified address of the recipient was not correct. You are recommended to complete this form and send it back with your reply to us.

Please do this within the period of one week - if we don't get your timely reply you will be paid your money back less 18%.
From Costco <manager@eeag.sakura.ne.jp>

Subject: Scheduled Home Delivery Problem

To:

Unfortunately the delivery of your order COS-0053845859 was cancelled since the specified address of the recipient was not correct. You are recommended to complete this form and send it back with your reply to us.

Please do this within the period of one week - if we don't get your timely reply you will be paid your money back less 18%.
Cyber Security

From: NETFLIX
Subject: We've temporarily suspended your account until you verify your details.
Date: 21/1/19, 4:09 am

To: [redacted]

NETFLIX

Your account has been suspended

Dear client,

We've temporarily suspended your account due to some issues in the automatic verification process.

For this reason we suspended your account, until you verify all required informations and update your payment method. We will provide all the steps you need to unlock your account. Please follow these instructions after you click on the link below.

UPDATE YOUR DETAILS

Follow these steps:

1. Login to your account.
2. Update your Billing informations.
3. Update your Payment method.

If you do not verify your account, your account will be deleted permanently.

Please help us to clear your status and unlock your account.

Thanks,

Netflix
Cyber Security

This email uses a display name of "NETFLIX" with a lower case 'L' character to replace the 'i'.

Your account has been suspended

Dear client,

We've temporarily suspended your account due to some issues in the automatic verification process.

For this reason we suspended your account, until you verify all required informations and
To:

- You were copied on an email and you don’t know the other people it was sent to.
- A generic greeting is used – not your name.
Cyber Security

Date: line

- Receive an email you would normally get during normal business hours, but it was sent at 3 a.m.
Subject: line

- The subject line of an email is not relevant or doesn't match the message content.
- An email about something you never requested or a receipt for something you never purchased.
Content of email

- Sender is asking you to click on a link or open an attachment to avoid a negative consequence
- You have an uncomfortable feeling, or it just seems odd or not logical.
From Costco <manager@eeag.sakura.ne.jp>

Subject: Scheduled Home Delivery Problem

To: 

Unfortunately the delivery of your order COS-0053845859 was cancelled since the specified address of the recipient was not correct. You are recommended to complete this form and send it back with your reply to us.

Please do this within the period of one week - if we don't get your timely reply you will be paid your money back less 18%.
The email is deliberately trying to get an emotional response from you.

Good or Bad
Hyperlinks (links)

• Look for misspellings
• Email contains hyperlinks asking you to take an action
• Text, images and buttons can contain malicious hyperlinks
From: Costco <manager@eeag.sakura.ne.jp>  
Subject: Scheduled Home Delivery Problem  

To:  

Unfortunately the delivery of your order COS-0053845859 was cancelled since the specified address of the recipient was not correct. You are recommended to complete this form and send it back with your reply to us.

Please do this within the period of one week - if we don't get your timely reply you will be paid your money back less 18%.
Unfortunately the delivery of your order COS-0053845859 was cancelled since the specified address of the recipient was not correct. You are recommended to complete this form and send it back with your reply to us.

Please do this within the period of one week. If we don't get your timely reply you will be paid your money back less 18%.
Attention:

Due to the recent cyber attack on our Social Security Administrative database, we advise that all United State SSN holders should update their SSN details for safety and security purpose.

We need your help to complete this security update by re-updating your information online.

CLICK HERE to proceed with your SSN Update

You will need to provide us with all information require.

Regards,

Social Security Administrator
United States of America
OH NO!
My Social Security profile has been recorded.

I have to CLICK the link and FIX it!
Phishing Voicemail Message

Greeting

Voicemail

+1 (260) 236-0301
Decatur, IN
July 25, 2019 at 9:37 AM

Transcription Beta
“This is an important message regarding your business on Google _________ or if you posted on your listing or lack of reviews is _________ your business online please call us at 800-259024 8/______ resolve this I mediate this is before is available to assist you Monday through Friday 9 AM to 6 PM Eastern standard time again that number is 800-259-0284 thank you...”

Was this transcription useful or not useful?

Speaker

Call Back

Delete

+1 (269) 313-2877
Saint Joseph, MI
Tuesday 0:08

Favorites Recents Contacts Keypad Voicemail
BREATHE

Cyber Security
THINK
Cyber Security

Social Security

Attention:

Due to the recent cyber attack on our Social Security Administrative database, we advice that all United State SSN holders should update their SSN details for safety and security purpose.

We need your help to complete this security update by re-updating your information online.

CLICK HERE to proceed with your SSN Update

You will need to provide us with all information require.

Regards,

Social Security Administrator
United States of America
Attention:

Due to the recent cyber attack on our Social Security Administrative database, we advise that all United State SSN holders should update their SSN details for safety and security purpose.

We need your help to complete this security update by re-updating your information online.

CLICK HERE to proceed with your SSN Update

You will need to provide us with all information required.

Regards,

Social Security Administrator
United States of America
Attention:

Due to the recent cyber attack on our Social Security Administrative database, we advise that all United State SSN holders should update their SSN details for safety and security purpose.

We need your help to complete this security update by re-updating your information online.

CLICK HERE to proceed with your SSN Update

You will need to provide us with all information require.

Regards,

Social Security Administrator
United States of America
• ALWAYS hover over any links (text, images and buttons). Is the address correct?
• Somewhere on your screen, you will see the URL of the link.
GROUP ORDER - SUBMIT ORDER

Scott,

Your group order 1346597 is nearing its close time and can be added to until Fri., Jun 7 10:00 AM.

Click here to review and submit your group order to the store.

The following invitees have not yet responded:
vsolanki@kiwanis.org, rchampney@kiwanis.org

Please do not reply to this email. It is not a monitored email address
Cyber Security

https://online.jimmyjohns.com/grouporders/2ae1b17d-01d7-4843-9702-6f8118b6c12c/status/
Cyber Security

https://www.example.com

- Protocol (scheme)
- Sub-domain
- Domain name
- Top level domain (TLD)
RED FLAGS – spoofing links

- http://actionelectronics.onmicrosoft.com
- Service@Amazen.com
- www.Micorsoft.com
- www.Youltube.com
Attachments

• ANY attachment you receive that you aren’t expecting is a RED FLAG.
Cyber Security

What do I remember?
Cyber Security

- Emotional response – good or bad
Cyber Security

- Emotional response – good or bad
- **STOP** – **BREATHE** – **THINK**
Cyber Security

- Emotional response – good or bad
- **STOP** – **BREATHE** – **THINK**
- **RED FLAGS** -
Cyber Security

- Emotional response – good or bad
- STOP – BREATHE – THINK
- RED FLAGS – Anatomy of email
Cyber Security

- Emotional response – good or bad
- **STOP – BREATHE – THINK**
- **RED FLAGS** – Anatomy of email
  - From
  - To
  - Subject
  - Date
  - Content
Cyber Security

- Emotional response – good or bad
- **STOP** – **BREATHE** – **THINK**
- **RED FLAGS** – Anatomy of email
  - From
  - To
  - Subject
  - Date
  - Content - spelling/grammar, links, attachments
Common sense approach

- Did I initiate this communication?
- Do I even have this account?
- Is this out of character for the sender?
- Do I have another way of confirming this email?
Common sense approach

When in doubt – DELETE the email.

If it's important, it will come back to you in another form – physical mail and/or phone call.
Cyber Security

Questions?