**Security Measures When Using the Internet**

Computers, cell phones, tablets, and other electronic equipment are not as private as we are led to believe. Safe guard your identification badges and passwords.

There is a possibility of sending misdirected e-mails, having cell phone conversations and sending texts with language we would not normally use if we were in front of the person. Be sure to always use the electronic device as if you are in the room with the person in which your e-mail, phone call or text is directed. Anonymity seems to make us braver and act differently than we normally would.

Internet Security Tips:

* Have an e-mail address that you use only with family, friends, relatives, peers and colleagues. Depending on the e-mail address or service provider, it can be traced back to your location.
* Use a general e-mail account like yahoo and Gmail for online activities such as Facebook, Group Chat, Newsgroups, Snapchat, Twitter.
* Do not fill in the personal profile sections in apps or webpages like Facebook, Group Chat, Newsgroups, Snapchat, and Twitter.
* Use strong passwords. One not easily guessed and of at least 10-12 characters.
* Adjust settings and filters to block unwanted messages.
* Choose your internet name and e-mail address wisely. Try not to identify who you are, your gender, or your location.
* Do not open attachments that seem peculiar or unexpected from e-mail addresses you know and don’t know. If not sure, call the person or send a new e-mail to the person to check to see it is from them.
* Set you internet browser security to high and be specific with the websites you visit. Unwanted visits to random websites can lead to unwanted messages and e-mails.
* Cyberbullying and cyberstalking is as dangerous as if it was in person.
  + Report problems to local IT personnel or on the forum in which the events started. You may need to contact your internet service provider.
  + If the cyberbullying and cyberstalking continue, contact your local police and let them know you are concerned about your safety.
* In the event, where laptops, tablets or phones are stolen, keep passwords and personal information in another location not on the electronic device.
* Search your name on the internet to see what comes up. Were you easy to find?
* Be wary of meeting someone in person you have met online whether through business or pleasure. Take precautions to protect your personal and physical security if you decide to go ahead and meet.

Today we need to be aware of the fraudulent phone calls, text messages, and e-mails known as phishing attacks where scammers try to steal your personal information and passwords. Thousands of phishing attacks are launched on a daily basis and unfortunately, they are most often successful in gaining your information. Remember these attacks can look like they are coming from someone you know. The scammer uses special software to pretend to be someone they are not.

Sample Messaging of Phishing Attacks:

* State in the e-mail or message they have noticed suspicious activity or log-in attempts.
* State there may be a problem with your account or your payment information.
* Ask you to confirm some personal information.
* Attach a fake document to the e-mail.
* Ask you to click on a link to make a payment.
* State you have won something or entitled to monies.
* Offer you discounts or rewards on products.

Protect your internet security by being kind to others and not trusting everyone. It is ok to investigate e-mails and ask questions if you are not sure. You are only one click away from a harmful situation if you don’t ask questions.

**Security Measures When Using the Internet – DISCUSSION RECORD**

**Agenda:**

* What online work activities are performed on the farm electronic devices?
* What is your internet security settings? Low, Medium or High?
* Do you know how to do this?
* Where are your passwords saved? Do you use the same password for everything?

Comments or safety concerns as a result of the discussion or observed since the last rally?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Follow-up to concerns raised at previous rally?  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Action Items?  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Near Miss/Incidents/Unsafe Acts/Conditions to Report?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Topics recommended for future Rallies: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Thank the rally members for their participation.**

**Quiz Answers:** 1. T, 2. T, 3. T, 4.d, 5. d

**TEST YOUR KNOWLEDGE**

1. Anonymity seems to make us braver and act differently than we normally would when online. True or False
2. Thousands of phishing attacks are launched on a daily basis and unfortunately, they are most often successful in gaining your information.

True or False

1. Computers, cell phones, tablets, and other electronic equipment are not as private as we are led to believe. True or False
2. Select the criteria below that would indicate you have set up a strong password:
   1. 10- 12 characters in length
   2. Not easily guessed
   3. No personal Info included such as birth date
   4. All of the above
3. Select the examples of phishing attack language below:
4. Ask you to confirm some personal info.
5. Attach a fake document to the e-mail.
6. Ask you to click on a link to make a payment.
7. All of the above

**Attendance RECORD**

\*This is to acknowledge that I understand and agree to actively participate in the safety meeting.

|  |  |
| --- | --- |
| **Print Name:** | **Signature:** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |