# Mini-Drill Program: Cybersecurity

Department or Unit:   
Leader conducting Drill:   
Date Drill conducted:

## Objectives

1. Define cybersecurity:
   1. Cybersecurity, also known as computer security or IT security, is the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide.Identify general information regarding spill kits (for those who have spill kits on the unit).
2. Identify what Phishing is:
   1. Phishing is the activity of defrauding an online account holder of personal information by posing as a legitimate company.
3. Identify the first steps that should be taken if you received a Phishing email:
   1. Don’t open emails, attachments or links asking for personal information (i.e. name, SSN, account numbers, login, passwords, etc.).
   2. If you ever receive a suspicious email requiring personal information or credentials, please call the IT Help Desk immediately at [fill in point of contact]
4. Identify ways you can protect yourself and your private information:
   1. Be suspicious of hidden URLs, even on your home computers (i.e. http://fakesite.ourfacility.com, etc.).
   2. Change your business and personal passwords periodically and make them complex.
   3. Check your financial accounts regularly for suspicious activity.
   4. Type [Secure] in the email subject box to encrypt and protect emails and attachments containing sensitive information being sent to external recipients through email. **Remember** - This is NOT necessary for internal emails sent within internal email network.

## Conducting the Drill

This drill can be conducted at huddles, staff meetings, or randomly in an area where staff members are gathered: break room, nursing station, etc. **This should take approximately 5-10 minutes.**

1. Introduce yourself and explain to the staff that you will be conducting a short mini-drill to increase awareness around cybersecurity.
2. Ask the following questions:
   1. Identify what Phishing is.
   2. Identify the steps that should be taken if you receive a Phishing email.
   3. Identify ways you can protect yourself and your private information.

### Upon drill completion

1. Record the names of individuals on the completion form.
2. Answer the questions included on the completion form.
3. Submit the completion form (hard-copy, email or through online survey):
4. Refer any additional questions to [fill in point of contact].

## Mini-Drill Survey

Were staff members able to identify what Phishing is?  
Yes No  
Comments:

Were staff able to identify the steps that should be taken if you receive a Phishing email?   
Yes No  
Comments:

Were staff members able to identify ways theycan protect themselves and their private information?  
Yes No  
Where is it located on your unit?

Please document names of staff members who participated in the February mini-drill to be entered in drawing for prizes (use back-side if necessary):

Additional Comments: