Safety Hour Discussion Pack

Topic: Secure passwords

Ask yourself, are your passwords easy to guess?

Purpose of the discussion:

To discuss why passwords are important and how they protect us and our organisation.

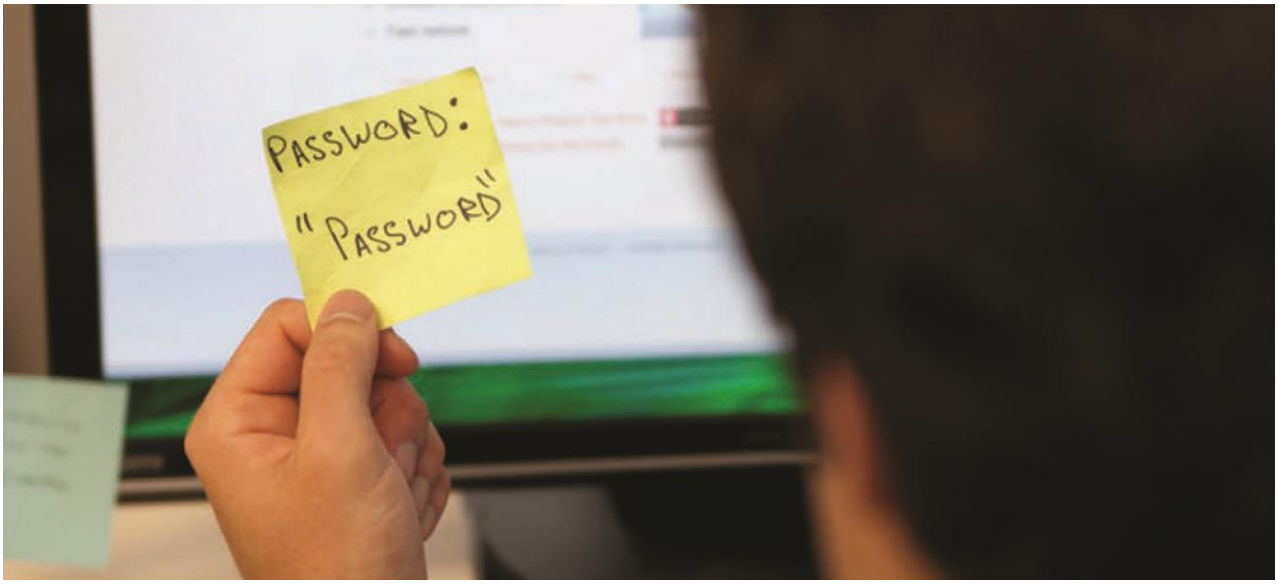
Before the session, if you haven't already done so, complete the mandatory security training via Oracle ebusiness OLM by searching for 'information security'. This will give you more information and help you to answer questions raised during the discussion.

Kick-off the discussion:

Start the discussion by saying –

We are asked for our passwords multiple times a day, they are there to protect systems and information. To keep access secure we are asked to make passwords complex and change them regularly and to never write them down.
We all know this is the right thing to do, but how many of us actually do it? Do we really consider the risks of not maintaining strong passwords?

This Safety Hour is part of a series based around 8 questions we should ask ourselves in order to work securely and understand the contents of our security policy and standards. We want to avoid security breaches or incidents which could impact the safe operation of the railway and the safety of our colleagues and customers.
Find out more about the 8 asks here: http://oc.hiav.networkrail.co.uk/SITES/SEC_CHAMPS/
Guide on creating strong passwords password best practice guide



Safety Hour Discussion Pack

Topic: Ask yourself, are your passwords easy to guess?

Discussion points: Use below to plan your facilitated discussion. Remember, you don't have to have all the answers – the role of the facilitator is to create an engaging discussion where everyone identifies and commits to solutions.

Discussion points	Supporting notes
Why do we need strong passwords?	**Who might want to hack our passwords in order to access our information and systems? What information might they want? What might they be able to do if they logged into our systems?** • What systems do we use, financial, HR, critical systems? • What sensitive or valuable information do we have access to - commercially valuable, reputationally damaging, of interest to terrorists? • Would you want everyone to see your records? How much you get paid? Where you live? **All these things are protecting by our passwords, our encryption is strong but not if the password is weak.** **How would you feel if someone accessed your personal phone or laptop?** • Would it be embarrassing? Damage your reputation? Financially harmful? • What could be done with that data? **We need to think of our professional devices in the same way.** **Key messages here are:** • **Strong passwords prevent theft, deletion or damage to our information assets and unauthorised access to our systems.** • **We should all be conscious of the value of our information and systems.**

Safety Hour Discussion Pack

Topic: Ask yourself, are your passwords easy to guess?

Discussion points: Use below to plan your facilitated discussion. Remember, you don't have to have all the answers – the role of the facilitator is to create an engaging discussion where everyone identifies and commits to solutions.

Discussion points	Supporting notes
What happens if we don't have strong passwords?	**You might have seen in the press about TalkTalk, Tesco Bank, Ashley Madison… Ask the group – has anyone had their data hacked?** • How did it make them feel? • Could it be because of a weak password? • If someone had your personal details could they guess your passwords? **Are the passwords you use for work as strong as your personal passwords? Are they the same passwords?** **What prevents you from having strong passwords?** • Too hard to remember? • Too many passwords? • Don't see the importance of having strong passwords? **Key messages here are:** • **A password for our systems should be just as strong as the ones you'd use to protect your personal information (such as internet banking).** • **Passwords can be broken using guessing (common password), educated guessing (by finding out information about the user) or using software to hack the password** • **You are a target for criminals because you work on our countries critical national infrastructure.**

Safety Hour Discussion Pack

Topic: Ask yourself, are your passwords easy to guess?

Discussion points: Use below to plan your facilitated discussion. Remember, you don't have to have all the answers – the role of the facilitator is to create an engaging discussion where everyone identifies and commits to solutions.

Discussion points	Supporting notes
What makes a password strong?	**Has anyone in the group got some top tips, a tactic they use to create strong complicated passwords they are able to remember?** **We can all improve by…** • regularly changing our passwords • not using one password for all logins. Make them system specific by including name of the system in password • including special characters, mixed cases, substitutions (3 for E, ! for I) • Do what works for you, make them memorable • A string of unrelated words can be a strong password **Key messages here are:** • **Never write down or share your password** • **You are responsible for other's actions if they are using your account.** • **Raise your concerns or report something insecure to AskSecurity@networkrail.co.uk or via close call.** • **For practical tips, take a look at the password best practice guide on the security champions sharepoint using the link on page 1.** **Has everyone completed their mandatory security training?** This can be done using the 'Information Security – Discussion Pack' Safety Hour on Safety Central, via a briefing by your line manager or completing the elearning using Oracle e-business by searching for 'information security' on OLM.

Safety hour based on one of the 8 Ask Yourself security questions.
Select those most relevant to you and if you have any questions or concerns about security or delivering this safety hour please get in touch.
Contact AskSecurity@networkrail.co.uk or search 'Security' on connect.
Use #AskSecurity to visit the Information Security group on Yammer.