Safety Hour Discussion Pack

Topic: Secure connections

Ask yourself, how do you know if the connection you're using is trusted?

Purpose of the discussion:

To discuss what acceptable use is and how it applies to our security at home and at work.

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 rely on internet connections to operate our infrastructure: we trust our corporate networks to protect our information. Do we also trust our home internet connection? What about public wifi? Do we consider the security of the internet connections we use?

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/

home safe plan

Ask yourself Ask security

Safety Hour Discussion Pack

Topic: Secure connections

Ask yourself, how do you know if the connection you're using can be trusted?

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 to know our connections are secure?	**Ask the group to discuss their thoughts on online security. What are the different ways we connect to the internet? How do we protect ourselves when using different connections?** • **Public?** – Wireless internet accessed in public places – coffee shops, airports, shopping centres etc. • **Home?** – Internet provided via a chosen supplier transmitted wirelessly. • **Work?** – Corporate networks provided by Network Rail accessed using authorised devices Using different connections requires different security considerations. All networks are vulnerable and can be used to access or damage the information and systems connected to them. **How could this type of attack lead to unsafe circumstances for us?** Has anyone experienced an incident of cyber crime? How did it effect you? Could it have impacted yours, your families or your colleagues safety? (Would you be focussed on your job if you had just had your bank account emptied?) **Key messages here are:** • **Our information has value. Consider the importance of where you work, make sure you're working in a safe and secure way, only using secure networks.** • **Be aware of the risks depending on where you are connecting and what you are doing online.** • **We are all a target for cyber criminals both personally and as Network Rail staff.**

Safety Hour Discussion Pack

Topic: Secure connections

Ask yourself, how do you know if the connection you're using can be trusted?

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 are the risks?	**We are all a target for cyber criminals. Being online, we put ourselves at risk, we work, email, bank and shop, relying on our connections to protect our information.** • Why would someone want to hack into our connections? • Who might target you personally? • Who might target us as an organisation? **Making sure internet connections are secure plays an important part in maintaining a safe railway. Do we understand the risks of different ways of connecting?** • **Public** – unauthorised people can intercept anything you are doing online, capturing your password, reading private emails, accessing your bank account. • **Home** –unauthorised people within range could be doing the following, use your bandwidth, use your download allowance, download inappropriate material, access sensitive information or hack into connected devices such as using the camera in your TV to spy on your family. • **Work** – we are a target for cyber attacks, criminals will try to damage or access our systems by exploiting staff to bypass our technical controls. **Key messages here are:** • **A secure connection protects our personal information and the systems and equipment critical for running our infrastructure.** • **We need trusted secure connections to operate our infrastructure and keep people safe.** • **Connecting to an insecure connection can open ourselves and our systems to attacks which could lead to an unsafe situation.**

Safety Hour Discussion Pack

Topic: Secure connections

Ask yourself, how do you know if the connection you're using can be trusted?

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 can we do to reduce the risks to ourselves and our organisation?	**What can we do? Ask the group to discuss their thoughts on online security? What do you do to protect yourself and your family?** • Public – Never trust a public connection with personal data or usernames and passwords. If in doubt, don't use the connection. • Home – Change the default admin password on your router, understand the risks of using wifi connected devices, they put your connection at risk and vulnerable to attack. • Work – Only use corporate networks, wifi (via the VPN) or data (3/4G) to connect our devices. Keep work devices for work use with a small amount of personal use to reduce the risk to you and the organisation. **Key messages here are:** • **Only use NR trusted networks or VPN when connecting NR devices and equipment.** • **Create a secure connection using our corporate VPN (Virtual Private Network) even if just surfing the internet at home. You can also protect your personal devices in the same way using a VPN provider.** • **Our IT systems are protected by our security controls but these can be compromised and made unsafe if the connection is not secure.** **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.

home safe plan