Safety Hour Discussion Pack

Topic: Cyber Security

Purpose of the discussion:

To discuss why Security is a top threat for Network Rail.

We already live in a digital world and will rely more and more on inter-connected systems and technology to deliver railway services in the future. Security impacts us as individuals as well as our railway. Security is linked to a safer railway and can safeguard performance.

Security is everyone's responsibility. To help protect our railway we all need to behave securely.

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 to you and how can you reduce them?	Let the team discuss how they can protect themselves and their families from cyber threat. Has anyone suffered from a cyber attack? What happened and what are they doing differently?? Key messages here are: • Be safe online, at home and work. Ask yourself, is this secure? Click with care and always browse safely. Never select links to/from un trusted sites. • Behave securely- Protect your identity, passwords and devices both at home and at work. Don't share personal information, protect company information and protect all your passwords whether at home or work.
What are the risks to your colleagues and how can you reduce them?	Let the team discuss how they can protect our buildings and systems. Is there anything they currently do, or don't do, that could make us vulnerable to an attack? Here's some examples of best practice : • Never share your password/s. • Always lock your screen when you're away from your desk, even if it is for a moment. Hit ENTER after, CTRL+ALT+DEL every time you leave your seat or press WINDOWS+L. • Never leave mobile devices unattended. If lost or stolen, report immediately. • Always wear your ID badge and/or have your Sentinel card ready for inspection. • Challenge suspicious behaviour, tail-gaiting and those without ID – contact the local security team or use the 'speak out' line if required

Safety Hour Discussion Pack

Topic: Cyber Security

Discussion points	Supporting notes
What are the risks to the railway and how can you reduce them?	**Respect our security measures** – don't tailgate or allow access to someone you do not know. Make sure access gates are locked. If challenging suspicious behaviour do remember that your personal safety is paramount. **Follow company policy and standards** – make sure you know the rules on email, social media, mobile devices etc. There are people you can ask if you are unsure. **Protect company information** – be careful how you handle removable media (USB sticks), think about what information you're emailing – is that the most appropriate way of sharing information? Always lock and secure devices when unattended or not in use.
Real examples of Cyber Security events that affected us and a security case study	Over 6,000 NR employee identities were stolen from HMRC and used as part of a credits fraud. Note: This is an historic loss for HMRC, additional compliance checks are in place A supplier's laptop containing NR pensions data was stolen. Fortunately no attack was made and the laptop was recovered. The information security team ran a simulated phishing scam to help raise awareness of online threats. More than 20% fell foul to the 'scam'

For further information:

Contact the Security team – AskSecurity@networkrail.co.uk

Watch 'Norm's Bad Day' - http://connect/communities/cyber-security/what-can-you-do.aspx