CYBERSECURITY

Source: The Walt Disney Company

WHAT DOES THIS MEAN AT DISNEY?

Global cybersecurity attacks are a frequent occurrence. How do we help protect Disney, our guests, and our businesses? We can be diligent in writing secure software, architecting secure systems and infrastructure, running security scans to test for weaknesses, repairing vulnerabilities of technical currency, and guarding our important data through encryption and responsible data handling. Additionally, we can help protect our Company by educating ourselves about attacks, being observant, and spreading awareness about cybersecurity threats and the ways we can protect ourselves.

Now that you've watched the Cybersecurity module, take some time to think about how you can take your learning further.

Reflection

Employee responsibility is the most important aspect of protection individuals can take. Most breaches involve an employee doing something that lets cybercriminals break into our network.

- Do you know how to spot a phishing attack?
- Do you know what do with a suspicious e-mail? (Answer: forward it to bademail@disney.com)

Group Discussion

Discussions are a great way to take your learning further by sharing it with others. Share the module and talk about what it means with others.

Here are some questions to get the conversation started:

- What was your initial reaction to what you heard?
- What is a key takeaway for our business?
- How do you think these ideas could be applied to our work?
- What vulnerabilities exist in our departments?
- How do we protect the company against threats?

Additional Resources

- 2014 Information Security Breaches Survey, UK Department for Business Innovation and Skills
- Interesting infographic shows security breaches are getting more costly
- TWDC Cybersecurity Resource site