Instructor Resource

Questions and answers for Security Guides, Ethics Guides, and Guide Guides

Table of Contents

[Security Guides 3](#_Toc459995351)

[Chapter 1 - Password Etiquette 3](#_Toc459995352)

[Chapter 2 - Evolving Security 5](#_Toc459995353)

[Chapter 3 - Hacking Smart Things 6](#_Toc459995354)

[Chapter 4 – Anatomy of a Heartbleed 7](#_Toc459995355)

[Chapter 5 – Theft by SQL Injection 9](#_Toc459995356)

[Chapter 6 - From Anthem to Anathema 11](#_Toc459995357)

[Chapter 7 – One-stop Shopping 13](#_Toc459995358)

[Chapter 8 - Digital is Forever 15](#_Toc459995359)

[Chapter 9 - Semantic Security 16](#_Toc459995360)

[Chapter 10 – EMV to the Rescue 18](#_Toc459995361)

[Chapter 11 – Selling Privacy 19](#_Toc459995362)

[Chapter 12 - Psst. There’s Another Way, You know… 20](#_Toc459995363)

[Ethics Guides 22](#_Toc459995364)

[Chapter 1 - Ethics and Professional Responsibility 22](#_Toc459995365)

[Chapter 2 – I Know What’s Better, Really 23](#_Toc459995366)

[Chapter 3 – Yikes! Bikes 25](#_Toc459995367)

[Chapter 4 - Free Apps for Data 27](#_Toc459995368)

[Chapter 5 - Querying Inequality 28](#_Toc459995369)

[Chapter 6 - Cloudy Profit? 29](#_Toc459995370)

[Chapter 7 – Dialing for Dollars 30](#_Toc459995371)

[Chapter 8 - Synthetic Friends 32](#_Toc459995372)

[Chapter 9 – Unseen Cyberazzi 33](#_Toc459995373)

[Chapter 10 - Securing Privacy 35](#_Toc459995374)

[Chapter 11 – Privacy vs Productivity: The BYOD Dilemma? 37](#_Toc459995375)

[Chapter 12 - Estimation Ethics 38](#_Toc459995376)

[Guide Guides 39](#_Toc459995377)

[Chapter 1 – Five-Component Careers 39](#_Toc459995378)

[Chapter 2 – Egocentric Versus Empathic Thinking 40](#_Toc459995379)

[Chapter 3 – Your Personal Competitive Advantage 42](#_Toc459995380)

[Chapter 4 – Keeping up to Speed 44](#_Toc459995381)

[Chapter 5 - Slick Analytics 46](#_Toc459995382)

[Chapter 6 – Is it Spying or Just Good Management? 48](#_Toc459995383)

[Chapter 7 – ERP and the Standard, Standard Bluprint 50](#_Toc459995384)

[Chapter 8 – Developing Your Personal Brand 52](#_Toc459995385)

[Chapter 9 – Data Mining in the Real World 54](#_Toc459995386)

[Chapter 10 – Phishing for Credit Cards, Identifying Numbers, Bank Accounts 56](#_Toc459995387)

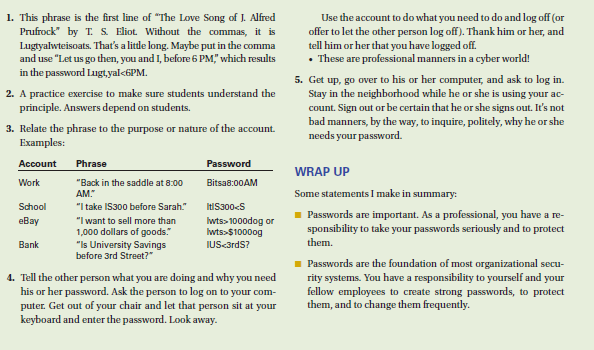
[Chapter 11 – Is Outsourcing Fool’s Gold? 57](#_Toc459995388)

[Chapter 12 – The Final, Final Word 59](#_Toc459995389)

# Security Guides

## Chapter 1 - Password Etiquette





## Chapter 2 - Evolving Security

Questions

1. This guide emphasizes how information security strategy has changed over the past two decades due to advancements in technology. What do these changes mean for you personally in managing and securing your own personal systems and data?

Private technology users encounter the same types of risks that companies encounter. If your tablet or smartphone is lost or stolen, the data on those devices can be compromised with minimal effort. If you happen to use Dropbox, this means that all of your personal photos, documents, financial statements, and even tax returns may be accessed by a third party. Furthermore, if you are tech savvy and happen to have a VPN set up to your home network, nefarious actors could access systems and other devices on your home network.

1. Take a few minutes to conduct an Internet search on insider threats. Besides some of the high-profile cases of employees stealing and selling or distributing corporate data, what other examples can you find?

Students will find a vast array of examples based on their search terms. The key point of this question is to help students recognize that insider threats are common and that the risks associated with insider threats are severe.

1. What kinds of collaboration tools have you used to complete class assignments and projects? Could these collaboration tools pose a risk to you? How?

Students have likely used file-sharing software like Dropbox to compile and access team resources. Dropbox users often forget to end shared access to folders and files when the project ends and thereby leave vulnerabilities open to any device linked to their Dropbox account if a former collaborator were to upload a malicious file. Students have also likely used Google Docs – other team members can easily access information shared in a Google Doc and disseminate that information to other friends or teams without the consent of the content creator.

1. How do you feel about the trend of companies using new technologies to monitor their employees? Would you want to work for a company that uses monitoring technologies? Why or why not?

The response to this question is clearly subjective and student responses will be mixed. Some students will likely encourage any measure that can be taken to secure the systems and data at their place of employment while others will consider these technologies an invasion of privacy.

1. Monitoring digital activity is not exclusive to the workplace. Internet service providers monitor your Web traffic and many Web sites monitor everything that you do while interacting with their site. What does this mean for users working from home? How might an ISP’s monitoring activities be a threat to corporations?

The main tension in information security used to be between security and accessibility. Today a new tension between security and privacy has emerged. Privacy is clearing being sacrificed in most digital environments and the implications of this trend are difficult to quantify. Privacy will be a perpetual issue as technology continues to become more and more pervasive over time.