New Mexico Broadband Program

Security and Safety in the Digital Age

Module 2

Protecting your Personal and Financial Security Online
Learning Outcomes

• Understand general guidelines for online security
  • Understand secure websites and passwords
  • Understand precautions needed for social media
• Understand how to avoid hacking, phishing, & identity theft
Internet security and safety

Most of us know that using the Internet can pose a potential threat to our online security and safety.
Understanding Internet security and safety can help us prepare and protect ourselves.
Threats usually involve other people gaining access to our personal or financial information.
Two guidelines for keeping personal and financial information secure:

1. Take basic precautions.
2. Don’t give information away!
Precaution: Don’t broadcast personal information such as your birthday, home address, or marital status unless it is required by the business you are engaging.
Precaution: Use secure websites that begin with https.
Secure websites show a gold lock somewhere on the website.
Precaution: Create strong passwords.
Strong passwords

Contain letters and characters
Contain symbols
Are 10 – 15 characters long
Interweave types of characters
Precaution: Change passwords frequently.
Social media sites are friendly, but still require that you take precautions.
Social media sites are public forums.
The information you post on your social media site should meet the “new friend” threshold.
Social media sites allow you to control who views your sites.
Setting controls on Facebook.
Hacker: One who accesses a computer system by circumventing its security system.
Protect against hacking: Update your operating system.
Protect against hacking: Turn your computer off when not in use.
Phisher: One who attempts to get secure information by impersonating a legitimate institution.
Protect against phishing: Do not respond!
Identity theft: According to the Federal Trade Commission, “identity theft ... [consists of] someone us[ing] your personal identifying information, like your name, Social Security number, or credit card number, without your permission to commit fraud or other crimes.”

http://www.ftc.gov/bcp/edu/microsites/idtheft//consumers/
Protect against identity theft: Keep your information private. Make it difficult to find.
Protect against identity theft: Monitor your accounts and billing information.
Protect against identity theft: Change your passwords frequently.
The online world is neither more nor less secure than other environments.
Review

• Keeping information private
  • Secure websites
  • Passwords
• Security and social media sites
• Hacking, phishing, and identity theft
We appreciate the time you spent with us. We hope to see you at the next training!

These materials were created collaboratively by the New Mexico Department of Information Technology, Fast Forward New Mexico, and the New Mexico State Library, under grants provided by the National Telecommunications and Information Administration. These materials are not to be used for profit.

Connecting you to a world of opportunities