CyberSecuring Your Home
Presented by: Dr. Debasis Bhattacharya, UH Maui College
Email: debasisb@hawaii.edu
Location of Presentation - http://maui.hawaii.edu/cybersecurity

Key Concepts:

• Basic Hygiene - Train family members in security principles, safety measures
• Active Defense - Actively guard and monitor your home network and cyber defenses
• Neighborhood Watch - Share common tips and tricks with others in your community
• Sensitive Information - What is it? Why you need to take care of it!
• Computer Scans - Automated way to check for SSNs. Check www.identityfinder.com
• Encryption - Ensure that nobody who has access to your data, can actually read it
• Cloud Storage - Usually unsecure but very convenient. Include Google Drive, Dropbox
• Social Engineering - Usually a combination of phone calls, letters, emails and SMS!
• Back-ups - Nothing can be secure in one place. So, backup and store in secure place
• Password Security - Usually, the main target. Hard to crack, easy to remember!
• Home Router - Key to keeping intruders away! Always use a password on the router
• Parental Controls - Control the nature of content viewed on your computers at home
• Filtering Content - Control what and when you can view online content in your home
• Secure Browsing - Critical for e-commerce or online banking. Check for https://
• Fake URLs - Often found in web sites that lead users to download ads and malware
• Public Computers - Often founds in hotel lobby, airports, Kinko’s. Always clear cache
• Safe use of Email - Avoid clicking on suspicious links, downloading attachments etc,
• Guard against SPAM - Most of Email is SPAM. Avoid downloading form SPAM emails
• Phishing - Entice users to part with sensitive information, based on emails, calls etc.
• Digital Millennium Copyright Act - Forbids downloads of illegal content - movies etc.
• Social Networking - Very popular with kids. Inherently dangerous for privacy
• Mobile Devices - Smart Phones are often the most used device for social networking
• Location Services - Tags your photos and web usage with your location coordinates
• Public Wireless Networks - Available at Starbucks, McDonalds. Watch for Sniffing