ACT - Proposed Outline/Topics for '21 Days to Tighter Internet Security'

Focus: Agency Owners, Managers, & Operations Officers

Goal of this initiative is to provide Independent Agents the resources needed to help them better protect the PII & PHI.
Note: This will supplement the Security Issues Pocket Guide, and other ACT Security & Privacy resources.
We will use blogs and videos to help educate and instruct agents on ways they can protect their data.

Proposed Topics:

1) Create a Security Plan
2) Create a Disaster Plan
3) Monitor Your Equipment *(use tools such as the CIS 'Cyber Hygiene' toolset)*
4) Install & Monitor Anti-Virus & Anti-Malware Software
5) Know what states your agency is selling insurance – Know the Data Breach Laws By State
6) Security Training; Primarily the Email '10-Second' Rule
7) Secure Your Email; Encryption, Selecting a solid Secure/Encrypted Email Product
8) Password-Protect Your Mobile Devices
9) How To Detect Phishing emails
10) Create/Secure/Manage Passwords
11) Set Passwords on ALL Machines
12) Set Machines to log off after a period of time
13) Encrypt Your Computers and other devices
14) Document Retention
15) Document Destruction
16) Secure Your VOIP
17) Secure Access – On a Need-To-Know-Basis Only
18) Secure Your Wireless Routers
19) Basics for a solid Business-Class Firewall
20) Verify Agent Access to Carriers Websites – Limit Access (Need to Know)
21) Understand your responsibility if you use Credit Cards
22) Know What Is Connected to Your Network – Map Your Devices
23) Update Your Operating System – Keep up with patches *(possibly use CIS 'Cyber Hygiene' toolset?)*
24) Get Rid of obsolete Machines (running obsolete systems – see above)
25) Microsoft Baseline Security Analyzer – How To
26) Microsoft's Enhanced Mitigation Experience Toolkit (**EMET**)
27) Backing up your data and your computers
28) *Other?*