



Information Security Best Practices for Everyone

Federal agencies and all types of businesses need security measures to combat threats to information security. Even if you were not affected by the recent data breach at the Office of Personnel Management, these best books, courses, and videos, can help you to protect yourself and your intellectual property at work.

Introduction to Information Security

This course examines corporate security and how it affects end users, along with the best ways to secure your work environment, whether you work in an office, on the go, or at home. This course also examines security issues surrounding e-mail, the Internet, and social engineering.

Using your Desktop Computer and Mobile Devices Safely

Protecting information and computer systems against malicious attacks is paramount for any organization, and every end user, regardless of their job role, has a responsibility to use their desktop computer and mobile devices safely. This course examines the types of threats that desktop computers and mobile devices may face, and effective ways to secure them.

Using E-mail, the Internet, and Social Media Safely in a Corporate Environment

This course examines the ethical use of e-mail, guidelines for using e-mail safely, and how to deal with issues as they arise. This course also examines social networking, social media, the proper use of the Internet at work, and the security issues that can arise from posting or discussing corporate information on social media sites.

The resources below work great on a tablet. Wi-Fi is recommended for the best experience. For more technical details, go to http://documentation.skillsoft.com/en_us/support/index.htm#45670.htm

Identity Theft For Dummies

Offering practical solutions to help you deter, detect, and defend against identity theft, this important book gives you the tools to recognize what information is vulnerable, minimize your risk, stay safe online, and practice damage control if your identity is compromised.

Protecting Your Identity: A Practical Guide to Preventing Identity Theft and its Damaging Consequences

Providing thorough, practical, help and advice about how to protect your identity, this book contains valuable guidance on what to do if your identity is stolen, and where to get further assistance.

Outsmarting the Scam Artists: How to Protect Yourself From the Most Clever Cons

Including accounts from people who have been scammed as well as tips from convicted con artists, this thoughtful book offers practical advice for consumers who want to protect their money as well as the financial assets of their parents and families.

The videos below are presented by Byron Hynes. Byron Hynes is an Enterprise Technology Strategist, author, trainer, and consultant. He is a Microsoft Certified Trainer (MCT) and holder of multiple Microsoft and Cisco certifications. He has designed and configured several large Exchange, Active Directory, Windows Server, and Remote Access/VPN deployments for military, commercial, and small business clients. He has spoken at several Microsoft conferences and events in Europe, Canada, and the US, and was awarded the Microsoft Most Valuable Professional (MVP) Award in the Windows (Security) category.

Security Essentials: Avoid Social Engineering Attacks

Social engineering attacks, such as phishing or e-mail fraud, aim to get your personal information. The United States Computer Emergency Readiness Team (US-CERT) warns against giving sensitive information to anyone unless you're sure they are who they claim to be. In this video, Byron Hynes provides some key tips to prevent computer crime from happening to you.

Security Essentials: Encrypt Your USB Sticks and Portable Media

You can encrypt your hard drives, portable media, memory cards, and USB sticks to prevent phishing and information theft. Encryption tools include BitLocker, a built-in Windows product, and TrueCrypt, which is a free download. In the video, Byron Hynes demonstrates how to access BitLocker and use TrueCrypt to create a virtual drive in which any data stored will be encrypted.

Security Essentials: Encrypting Your Wireless Networks

It's important to protect confidential information transmitted across a wireless network from being accessed by others. You can use various methods of network encryption, such as WEP or WPA2, to secure a wireless private network. In this video, Byron Hynes creates an ad hoc wireless network and uses WPA2-Personal encryption to secure it.

Security Essentials: Enhance Your Privacy on Social Networks

Most social networks, such as Twitter, LinkedIn, Yammer, Foursquare, and Facebook, offer varying levels of privacy that enable you to control your online privacy and reputation. In this video, Byron Hynes uses the Privacy Settings tab on Facebook to customize the privacy levels for his profile and the ads, apps, and web sites that run on his profile.

Security Essentials: General Concepts

There are a number of ways you can protect your computer from security threats. In this video, Byron Hynes discusses the steps you can take to safeguard data.

Security Essentials: Improve Security by Running as a Non-Admin

Windows provides several ways to improve system security, such as the User Account Control feature or performing your day-to-day operations as a non-administrator, depending on your version of Windows. In this video, Byron Hynes uses the User Account Control feature and creates a new user that is not a member of the Administrators group to improve the security on a system.

Security Essentials: Recognizing E-mail Scams

E-mail scams, sometimes called phishing or fraud, exist to get your money or personal information. The United States Computer Emergency Readiness Team (US-CERT) provides key steps to avoid e-mail fraud, such as filtering spam and using antivirus software and a firewall. In this video, Byron Hynes discusses some specific things that you can do to recognize a fraudulent e-mail.

Security Essentials: Transfer Files Securely

It's important to ensure confidential files are transferred securely via e-mail. You can use a third-party service to encrypt files, or encrypt files yourself using tools such as 7-Zip or WinRAR. In this video, Byron Hynes uses WinRAR to encrypt a compressed file, assign a password, and encrypt the filenames to ensure they stay protected in transit.

Security Essentials: Use Automatic Updates

Automatic Updates keep your system up to date and resilient against the most common and newest threats. Most major vendors, such as Microsoft, Apple, and Google, have a secure automatic updating function built into their software. In this video, Byron Hynes demonstrates how to configure the Windows Update feature.

Security Essentials: Use Microsoft Security Essentials

You should use antimalware or antivirus software to protect your computer against cyber attacks. Microsoft Security Essentials is a free antivirus program for standalone systems or small organizations using Windows. In the video, Byron Hynes uses Security Essentials to protect his computer against virus attacks.

Security Essentials: Using Good Passwords and Managing Them

It's important to use good passwords for digital commerce and to protect your identity and confidential information. Good password practices include using passphrases or randomly generated strong passwords, using different passwords for different systems, and storing passwords safely. In the video, Byron Hynes uses good password practices to create strong passwords and store them in a password vault.

Follow us on Twitter [@AgLearnToday](https://twitter.com/AgLearnToday)



[AGLEARN.USDA.GOV](https://www.aglearn.usda.gov)

