IRS Security Awareness Tax Tips

Courtesy of Texas A&M Payroll Services and Financial Management Operations Accounting Services

The following are highlights provided from the IRS website; please visit each webpage for complete details.


Tips to Protect Your Personal Information While Online
https://www.irs.gov/uac/Tips-to-Protection-Your-Personal-Information-While-Online
- Give personal information over encrypted websites only (look for “https” at the beginning of the web address)
- Protect passwords (longer, tougher to crack; 12 characters ideal for most home users)
- Don't assume ads or emails are from reputable companies (type company/product name into search engine with terms like “review,” “complaint,” or “scam”)
- Don't overshare on social media
- Back up your files
- Save your tax returns and records

Tips for Using Credit Bureaus to Help Protect Your Financial Accounts
- www.Equifax.com/CreditReportAssistance; 888-766-0008
- www.Experian.com/fraudalert; 888-397-3742
- www.TransUnion.com/fraud; 800-680-7289

Talk to Your Family about Security Online and at Home

What You Need to Know to Protect Your Passwords
New protections for in place for the 2016 tax season include:
- 8 or more characters, including upper case, and lower case letters as well as numbers and a special character
- New features include a timed lockout and limits on unsuccessful log-in attempts
- Must complete 3 security questions
- Tax software partners must verify email addresses

Seven Steps for Making Identity Protection Part of Your Routine
- Read your credit card and banking statements carefully and often
- Review and respond to all notices and correspondence from the Internal Revenue Service
- Review each of your three credit reports at least once a year
- Review your annual Social Security income state for excessive income reported
- Read your health insurance statements
- Shred any documents with personal and financial information
- IRS direct deposit is safe and secure and places your tax refund directly into the financial account of your choice

Don’t Take the Bait; Avoid Phishing and Malware to Protect Your Personal Data
- Do not click on links – go directly to website instead
- Beware of phishing scams asking you to update or verify your accounts
- To avoid malware, don’t open attachments in emails unless you know who sent it and what it contains
- Download and install software only from websites you know and trust
- Use security software to block pop-up ads, which can contain viruses
- Ensure your family understands safe online and computer habits

Seven Tips to Protect Your Computer Online
https://www.irs.gov/uac/Seven-Tips-to-Protection-Your-Computer-Online
- Understand and use security software
- Allow security software to update automatically
- Look for the “s” for encrypted “https” websites
- Use strong passwords
- Secure your wireless network
- Be cautious when using public wireless networks
- Avoid phishing attempts

Texas A&M Information Technology and Human Resources
…educating employees about the Identity Protection Campaign

Learn more: http://employees.tamu.edu/spotlight/identity-protection-campaign