## Sample article for organizations to use to reach customers (551 word count)

*Post the following article on your websites and/or use in other communication vehicles to help your customers.*

---

## Simple steps to keep your online data safe

During the holiday shopping season, shoppers are looking for the perfect gifts. At the same time, criminals are looking for sensitive data. This data includes credit card numbers, financial accounts and Social Security numbers. Cybercriminals can use this information to file a fraudulent tax return.

There are a few simple things you can do to protect your identity and personal information online. Following these steps can also help you protect your tax return and refund in 2018:

- Shop at familiar online retailers. Generally, sites with an “s” in “https” at the start of the URL are secure. You can also look for the “lock” icon in your browser’s URL bar. That said, some criminals may get a security certificate, so the “s” may not always mean a site is legitimate.

- Avoid unprotected Wi-Fi. Users should not do online financial transactions when using unprotected public Wi-Fi. Unprotected public Wi-Fi hotspots may allow thieves to view transactions.

- Learn to recognize and avoid phishing emails that pose as a trusted source. These emails can come from a source that looks like a legitimate bank or even the IRS. These emails may include a link that will take you to a fake website. From there, the thieves can steal your username and password.

- Keep a clean machine. This includes computers, phones and tablets. You should install security software to protect against malware that may steal data. This software also protects against viruses that may damage files.

- Use passwords that are strong, long and unique. Experts suggest a minimum of 10 characters. Use a combination of letters, numbers and special characters. Use a different password for each account.

- Use multi-factor authentication when available. Some financial institutions, email providers and social media sites allow you to set your account for multi-factor authentication. This means you may need a security code, usually sent as a text to your mobile phone, in addition to a username and password.

- Sign up for account alerts. Some financial institutions send email or text alerts to an account holder when there is a withdrawal or change to their accounts. Generally, you can check your account profile to see what added protections may be available.

- Encrypt sensitive data and protect it with a password. This includes financial records, tax returns or any personal information on your computer. You should also back up important data to an external source. When disposing of a computer, mobile phone or tablet, make sure you wipe the hard drive of all information before trashing.

For more information, visit Taxes.Security.Together on IRS.gov.

Date: December 18, 2017

---

***NOTE TO EDITOR:*** Below are links to help taxpayers find the information they need.

**IRS.gov**

- IRS Tax Tip 2017-82

**On Twitter? Send these Tweets:**

- #TaxSecurity: If you get rid of a computer, mobile phone or tablet, #IRS recommends that you first wipe the hard drive. https://go.usa.gov/xnNZ6
- #TaxSecurity: #IRS reminds you to avoid unprotected & public wi-fi hotspots that may let thieves see your activity. https://go.usa.gov/xnNZ6
- #TaxSecurity: #IRS suggests that you back up your important data to an external source such as an external hard drive. https://go.usa.gov/xnNZ6