



## Taxpayers Should Protect Data All Year Round

---

With the online holiday shopping season in full swing, it's the perfect time for all taxpayers to take steps to protect their identities and personal data. The year, the IRS kicked off this annual event with National Tax Security Awareness Week. The IRS partnered with state tax agencies, the tax industry and other groups across the country to encourage all tax payers to think about data protection.

While the week is over, information on these five topics remains relevant year-round:

### Eight Steps to Keep Online Data Safe

Anyone with an online presence can do a few simple things to protect their identity and personal information. Following these eight steps can also help taxpayers protect their tax return and refund in 2018:

- Shop at familiar online retailers.
- Avoid unprotected Wi-Fi.
- Learn to recognize and avoid phishing emails that pose as a trusted source.
- Keep a secure machine.
- Use passwords that are strong, long and unique.
- Use multi-factor authentication when available.
- Sign up for account alerts.
- Encrypt sensitive data and protect it with a password.

### Recognize Phishing Email Scams

The IRS reminds people to be on the lookout for new, sophisticated email phishing scams. These scams not only endanger someone's personal information, but they can also affect a taxpayer's refund in 2018. Even if an email is from a known source, people should use caution because cybercrooks are very good at mimicking trusted businesses, friends and family.

### Five Steps Data Breach Victims Can Take

People who are the victim of a data breach should consider these five steps to help protect their sensitive information that can be used on a tax return:

- Determine what information the thieves compromised.
- Consider taking advantage of credit monitoring services offered to victims.
- Place a freeze on credit accounts to prevent access to credit records.
- Reset passwords on online accounts.
- Use multi-factor authentication when available.

## Thieves Use W-2 Scam, to get Employee Data

The IRS warns the nation's business, payroll and human resource communities about a growing W-2 email scam. Criminals use this scheme to gain access to W-2 and other sensitive tax information that employers have about their employees. The IRS recommends that all employers educate employees about this scheme, especially those in human resources and payroll departments.

## Five Signs of Small Business Identity Theft

Business filers should be alert for signs of identity theft. They should contact the IRS if they experience any of these issues:

- The IRS rejects an e-filed return saying it already has one with that identification number.
- The IRS rejects an extension to file request saying it already has a return with that identification number.
- The filer receives an unexpected tax transcript
- The filer receive an IRS notice that doesn't relate to anything they submitted.
- The filer doesn't receive expected or routine mailings from the IRS.

## More Information Available at IRS.gov

- Protection: Prevention, Detection and Victim Assistance
- Small Business Information Security: The Fundamentals (from the National Institute of Standards and Technology)
- Resources for Small and Midsize Businesses (from the United States Computer Emergency Readiness Team)
- Subscribe to IRS Tax Tips to receive regular email alerts from the IRS



1000 Essington Road,  
Joliet, IL 60435

(815) 773-2312 – Paul  
(815) 773-2313 – Rhonda  
(815) 725-2914 – Corey  
(815) 729-3841 – Margaret

Fax: (815) 773-0658

Email: [invest@gantzertinvco.com](mailto:invest@gantzertinvco.com)

Website: [gantzertinvco.com](http://gantzertinvco.com)