Small security measures that make a big difference when it comes to online safety

IRS Tax Tip 2021-179, December 3, 2021

Cybercrime is a constant concern in the online world which means everyone must be mindful of risks when they share devices, shop online and interact on social media. While this may seem overwhelming, it doesn't have to be. A few small security measures can lower the risk of exposure to online safety threats.

Beware of sharing personal information

No one should reveal too much information about themselves. People can keep data secure by only providing what is necessary. This reduces online exposure to criminals. For example, birthdays, addresses, age and especially Social Security numbers are some things that should not be shared freely. In fact, people should not routinely carry a Social Security card in their wallet or purse. Taxpayers should only share government issued ID after first verifying the nature of the request by contacting the agency or visiting the agency's website. If someone calls requesting personal or financial information, verify their request separately, otherwise hang up and report the contact.

Protect personal data

Adults should advise young users to shop at reputable online retailers. They should treat personal information like cash and shouldn't leave it lying around.

Use security software

People should make sure their security software such as anti-virus, and firewalls is always turned on and can automatically update. They should regularly backup and encrypt sensitive files stored on computers. Sensitive files include things like tax records, school transcripts and college applications. They should use strong, unique passwords for each account and enable two-factor or multi-factor authentication for online accounts where possible. They should also be sure all family members have comprehensive anti-virus protection for their devices, particularly on shared devices.

Know the risk of public Wi-Fi

Connection to public Wi-Fi is convenient and often free, but it may not be safe. Criminals can easily steal personal information from these networks. Always use a virtual private network when connecting to public Wi-Fi.

Learn to recognize and avoid scams

Everyone should be aware of common scams. Criminals use phishing emails, threatening phone calls and texts to pose as IRS employees or other legitimate government or law enforcement agencies. People should remember to never click on links or download attachments from unknown or suspicious emails.

Be aware of compromised accounts

Suspicious contact may appear to come from someone the user knows who has had their online accounts such as email, or social media, compromised by a criminal; meaning the account is theirs, but they didn't send the request.

More Information

- Publication 4524, Security Awareness for Taxpayers PDF

Subscribe to IRS Tax Tips

Page Last Reviewed or Updated: 03-Dec-2021