www.sa18.org November 2016

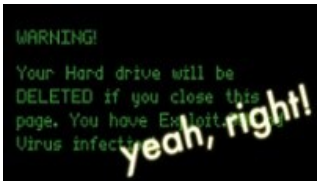
Online Shopping Safety Tips

Online shopping has taken over the consumer world and completely transformed the way that companies do business and how shoppers purchase goods. However, with that convenience and accessibility comes the potential for increased risk.

Adults in their golden years did not grow up with the Internet so they have been easy targets for fraud and identity theft mostly because they are so trusting or simply misinformed about how to safely shop online. Fortunately, there are many easy steps you can take to ensure your peace of mind.

- **Shop from secure retailers only.** Shop online from websites that begin with https rather than just "http." The "s" means secure and those sites have an added layer of data protection to ensure your information is transmitted directly to the retailer.
- **Use a credit card to shop online, not a debit card.** When you use a credit card, you essentially are spending the bank's money–not your own, as you are with a debit card-meaning that banks will likely fight fraudulent charges more aggressively.
- **Buy from secure companies that require a CVC code during checkout.** Companies that require the three or four digit code on the back of your credit card often have higher fraud-control policies and typically work with payment processors that have stringent fraud-protection control.
- **Protect access to your credit card information.** Don't allow anyone other than immediate, trusted family members to make purchases on your behalf using your credit/debit card. Don't send or store credit card information via emails or on unprotected sites.
- **Set up spending alerts.** A great way to reduce your risk of online shopping fraud is to set spending alerts on your credit card. Consider setting up an email or text alert to notify you when more than $500 is spent at any particular store or online site, so you are aware of any large purchases that are made instantly. Most banks have this easy to set-up feature.
- **Avoid making any purchases from pop-up windows or emails.** Visit store sites directly for products you're interested in. A common scam involves placing links into emails that appear to click through to shopping sites. You find out they are fraudulent after submitting your payment information and will never receive the items you ordered.
- **Avoid giving out your Social Security number unless absolutely necessary.** Banks, utility companies and health care providers might need this number but make sure you are the one initiating the request that warrants the SSN request.

Tech Support Scam



Bad guys are coming up with new ways to scam you out of your money all the time. Their latest trick is a Tech Support scam that puts a big warning screen on your computer, claiming that if you do not call the support number, your whole hard disk will be deleted in 5 minutes. A warning audio tone is also played in the background, which again warns the user that their system is infected.

There are variations of this scam that claim they are your Internet Service Provider, or claim to be Microsoft and you need an urgent update you need to call in for, or they show you a blue screen that claims your computer needs to be repaired. There is always a number to call, and these scammers will try to put hundreds of dollars on your credit card.

Don't fall for it! If you see error messages on your work computer screen, follow policy and contact your IT person. If you see this on your home computer, ignore the message! Do not call the fake tech support number!

New IRS Social Engineering Scam

There is a new IRS scam making the rounds. They send you a phony IRS CP 2000 Form and claim the income reported on your tax return does not match the income reported by your employer. This is meant to get you worried. To confuse you further, the bad guys claim this has something to do with the Affordable Care Act.

You might receive emails with attached phony forms, text messages and even live calls to your phone about this! You need to know that the IRS will never initiate contact with you to collect overdue taxes by an email, text message or phone call.

If you get any emails, text messages, old-time snail mail or even phone calls about this, do not click on anything, do not open attachments, do not reply and if it is a call, hang up the phone. If you receive a CP 2000 Form in the mail and doubt it is legit, you can always call the IRS at 1-800-366-4484 to confirm if it's a scam.