CLICK THIS. NOT THAT.

Do's and Don'ts for Safeguarding Your Personal Identity Online

Personal identity crimes are on the rise. In fact, according to the Federal Bureau of Investigations (FBI) identity theft remains among the top five internet crimes. Even more disturbing? A recent 2021 Trends in Identity reportfrom the Identity Theft Resource Center (ITRC) said that a full 50 percent of the incidents were the result of sharing personal identification information (PII) with the cyber criminals and led to these alarming statistics:

40% of identity theft resulted in financial account misuse

37% of account takeovers were with bank/financial accounts

36% of new account fraud was with credit cards

With criminal activity on the uptick and online holiday shopping right around the corner, it is important to remain vigilant against cyber criminals who want to steal your personal data. (And your holiday spirit.)

Do you know what to do – and what not to do – to stay cyber safe?

AHT INSURANCE
A BALDWIN RISK PARTNER

Do's and don'ts from the U.S. Cybersecurity & Infrastructure Security Agency (CISA) and other industry sources that can help you avoid becoming a victim of personal identity theft:

WHEN ONLINE SHOPPING

- Shop with reputable retailers. Look for "https" in URLs when you shop online so you know your information is encrypted
- Make sure the closed padlock icon is in the correct spot for your browser
- Avoid public WI-FI where hackers can gain access to the websites on which you shop and steal your data
- Shop at home or in a private setting where no one (or camera) could be watching you, without your knowledge
- Check your shopping app settings and confirm that it keeps your data secure
- Check bills carefully for errors or charges you did not make and report any issues
- Use a credit card with a low spending limit for online purchases
- Be skeptical of urgent emails that request personal data, such as: driver's license number, passport image, credit card account, etc.
- Respond to questions from an online retailer by going to their website or calling them on the phone
- Trust your instinct if a deal seems "too good to be true"

- Conduct transactions on websites that only have "http" in their URL
- Be fooled by "fake" padlock icons that are on a website…but in the wrong location for your browser
- Use free public WI-FI or websites that retain your banking, school, social media, or other confidential information
- Forget to disable "save password" option, log out when done, and delete browsing history
- Use a debit card connected to your bank account
- Share personal data electronically before you confirm the retailer is legit
- Directly reply through an email that they send you asking for account information or other credentials
- Forward any suspicious emails to others

WHEN MAKING HOLIDAY DONATIONS

- Contact the charitable organization personally to make your donation

- Give personal financial information to an unknown phone solicitor

WHEN CHECKING EMAIL

- Only open messages that are from those you know or are expecting
- Beware of embedded links or attachments
- Delete any emails that seem suspicious, have poor spelling or grammar, generic greetings, or need urgent action

- Click on unverified links in email messages or assume all links are safe to click

WHEN MANAGING YOUR SYSTEM

- Install anti-virus and anti-spyware protection on your computer
- Update security apps and software on a regular basis
- Erase and destroy your hard disk if you are getting a new computer
- Use strong, unique passwords/phrases for every online account you have; do not share them with anyone
- Consider using a password manager to create and remember passwords

- Ignore security patches
- Donate an old computer or bring it to a recycling center without completely removing everything from the hard drive first
- Default to using the same password for every website or account login
- Click “remember my password” on web login screens

Shopping, gifting, and donating online can be fast, convenient, and efficient. Just make sure it's safe, too!

CONSIDER CYBER INSURANCE

Typically available as an addition to your homeowners insurance policy, personal cyber insurance can cover a wide array of cybercrimes, ranging from cyber and ransomware attacks to data breaches and online fraud. Since all policies are different, it's important to discuss your specific needs and situation with your insurance broker and understand what's covered, what's not, and available coverage limit options.

For more tips about how you can keep your personal data secure, particularly during the upcoming holiday season, contact us today.

AHTINS.COM | 800.648.4807

AHT INSURANCE
A BALDWIN RISK PARTNER