2 MIN GUIDE:

Student Identity Theft

For many students, College is the first foray into the adult world and it's responsibilities

The Under 29 year old demographic comprised 24% of Identity Theft complaints to the FTC

Students often share passwords and PIN codes with friends

49% of college students receive applications for credit cards on a daily or weekly basis.

30% of all students simply throw away received applications without destroying them.

30% of students rarely, if ever, balance their checking accounts or reconcile their credit cards statements.

48% of all college students have had grades posted "anonymously" by Social Security number.

Many College students are opening financial accounts for the first time

Students are massive users of smart phones and tablets. Mobile = Danger. Students often use unsecured wireless networks when surfing the web

98% of college students use social media on a daily basis. We share huge amounts of information there, not always wisely or securely!

Kids love free!!! Whether its a coupon, game download, video, all of these are potentials for Phishing attacks where malware can be downloaded inadvertently.

resolution
Your Identity at Risk, Our Solutions at Work™

So What Can We Do to Be Safer...

- Checkbooks, credit card statements and other personal papers should be locked securely. Don't carry your Social Security card in your wallet or purse. Lock it up.

- Discarding papers containing personal information, such as bank account numbers, credit card numbers or a Social Security number, by merely throwing them in the trash is an invitation to dumpster diving identity thieves to gather the trash and turn it into their gold. Shred!

- DO set up passwords on mobile devices. DO NOT share them. The best passwords contain a long mix of small letters, capital letters and symbols.

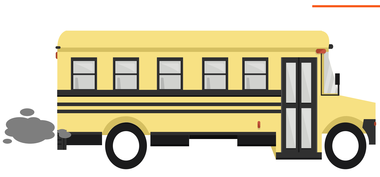
- Identity thieves make available free apps filled with malware. College students should be careful about where they get their apps and stay with sources that they know are legitimate, such as Apple's App store.

- Students may receive a message on their Facebook account telling them that they have to click on a link to see a startling video. The message may appear to be from a friend, but it often is from an identity thief who has hacked into the friend's account so that the malware tainted message appears to come from the friend when, in fact, it is from the thief. Don't download attachments or click on links unless you are positive that they are legitimate.

- College students often use WiFi in coffee houses, malls and other public places with little concern that the WiFi that they are using may be set up by the identity thief at the next table rather than the legitimate WiFi for the location. Check that your WiFi environment is legit and secure.

- College students often make purchases online and, for convenience, may leave their credit cards on file with the particular websites that they frequently use. This is a mistake.

- Don't store personal information on your laptop or smart phone. Limit the information you share on social media.



Hop on board and join us to keep our kids safer! Click on the button below to to learn more and watch our short animated video ...

Student Identity Theft...
Click to Learn More

resolution
Your Identity at Risk, Our Solutions at Work™