

## **Safeguard Your Student and Personal Information**

### **HOW IDENTITY THEFT HAPPENS**

**There are many ways that criminals can obtain your personal information. For example they:**

- Steal wallets and purses containing your identification
- Steal your mail, including your bank and credit card statements
- Rummage through your trash to get your personal data
- Find personal information in your home
- Use personal information you share on the Internet
- Scam you, often by email, by posing as legitimate companies
- Steal files or bribe employees who have access to files with your information
- Obtain your credit report by posing as a landlord or employer
- Request a copy of your birth certificate from the county recorder's office

### **REDUCE YOUR RISK**

#### **How can I protect myself from identity theft?**

The first step to prevent identity theft is awareness of how and when you use your personal information. By keeping close tabs on your personal information, you can reduce your chances of becoming an identity theft victim. Let's start with credit cards.

- Memorize your Social Security number and passwords. Don't record your password on papers you carry with you.
- Don't use your date of birth as your password.
- Shred pre-approved credit applications and other financial documents before discarding them.
- Order credit reports every year from each of the major credit reporting agencies and thoroughly review them for accuracy.
- Never give personal or financial information over the phone or Internet unless you initiated the contact.
- Don't carry your Social Security card or birth certificate with you.
- Report lost or stolen credit cards immediately.
- Check your monthly credit card and bank statements for unusual activity.
- Use a firewall program on your computer, especially if you leave your computer connected to the Internet 24 hours a day.
- Do not download files sent to you by strangers or click on hyperlinks from people you don't know.

Students applying for or using student loans should also:

- Use caution when using commercial financial aid services over the Internet or telephone. U.S. Department of Education services are free and password-protected. Before deciding to use a for-fee financial aid advice service, visit the [Looking for Student Aid site](#).

- Apply for federal student aid at [www.fafsa.ed.gov](http://www.fafsa.ed.gov). After completing the Free Application for Federal Student Aid (FAFSA) electronically, remember to exit the application and close the browser.
- Don't reveal your PIN to anyone, even if that person is helping you fill out the FAFSA. The only time you should use your PIN is on secure ED systems.
- Shred receipts and copies of documents with personal information if they are no longer needed.
- Review your financial aid award documents and keep track of the amount of student aid you applied for and have been awarded.
- Report all lost or stolen student identification immediately.

### **WHAT TO DO IF YOU ARE A VICTIM OF IDENTITY THEFT**

If you suspect that your personal information has been misused to commit fraud or theft, act immediately, and keep a detailed record of your conversations and correspondence (Including what was said, the name of the person who called, and from what number the call originated). Your first three steps should be:

**FIRST**, contact the fraud departments of each of the three major credit bureaus:

- **Equifax**: To order your report, call: 1-800-685-1111 or write: P.O. Box 740241, Atlanta, GA 30374-0241 To report fraud, call: 1-800-525-6285 or write: P.O. Box 740241, Atlanta, GA 30374-0241
- **Experian**: To order your report, call: 1-888-EXPERIAN (397-3742) or write: P.O. Box 2104, Allen TX 75013 To report fraud, call: 1-888-EXPERIAN (397-3742) or write: P.O. Box 9532, Allen TX 75013
- **TransUnion**: To order your report, call: 800-916-8800 or write: P.O. Box 1000, Chester, PA 19022. To report fraud, call: 1-800-680-7289 or write: Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

**SECOND**, close the accounts that you know or believe have been tampered with or opened fraudulently.

**THIRD**, file a police report with your local police or the police in the community where the theft took place.

If you become a victim of identity theft involving federal education funds or suspect that your student information has been stolen, contact:

- **U.S. Department of Education, Office of Inspector General Hotline**  
Email: [oig.hotline@ed.gov](mailto:oig.hotline@ed.gov), phone: 1-800-MISUSED (1-800-647-8733).

For more information or to report identity theft that does not involve federal education funds, visit the following sites:

- **Federal Trade Commission**, 1-877-IDTHEFT (1-877-438-4338)
- **Social Security Administration**, 1-800-269-0271
- **National White Collar Crime Center**

## OTHER SECURITY INFORMATION

### General Security Tips

- Protect your personal information. It's valuable.
- Know who you're dealing with.
- Use anti-viral software and a firewall, and update both regularly.
- Make sure your operating system and Web browser are set up properly and update them regularly.
- Protect your passwords.
- Back up important files.
- Learn who to contact if something goes wrong online.

### Spam Scams

- Protect your personal information. Share credit card or other personal information only when you're buying from a company you know and trust.
- Know who you're dealing with. Don't do business with any company that won't provide its name, street address and telephone number.
- Take your time. Resist any urge to "act now" despite the offer and the terms. Once you turn over your money, you may never get it back.
- Read the small print. Get all promises in writing and review them carefully before you make a payment or sign a contract.
- Never pay for a "free" gift. Disregard any offer that asks you to pay for a gift or prize. If it's free or a gift, you shouldn't have to pay for it. Free means *free*.

### Phishing

- Don't reply to email or pop-up messages that ask for personal or financial information, and don't click on links in the message. Don't cut and paste a link from the message into your Web browser – phishers can make links look like they go one place, but they actually send you to a different site.
- If you are concerned about your account, contact the organization using a phone number you know to be genuine, or open a new Internet browser session and type in the company's correct Web address yourself.
- Use anti-virus software and a firewall, and keep them up to date.
- Don't email personal or financial information.
- Review credit card and bank account statements as soon as you receive them to check for unauthorized charges.
- Be cautious about opening any attachment or downloading any files from email you may receive, regardless of who sent them.
- Forward spam that is phishing for information to [spam@uce.gov](mailto:spam@uce.gov) and to the company, bank, or organization impersonated in the phishing email. You also may report phishing email to [reportphishing@antiphishing.org](mailto:reportphishing@antiphishing.org).

- The Anti-Phishing Working Group, a consortium of ISPs, security vendors, financial institutions and law enforcement agencies, uses these reports to fight phishing.
- If you've been scammed, visit the Federal Trade Commission's Identity Theft website at <http://www.consumer.gov/idtheft>.

Resource: [OnGuard Online](#)