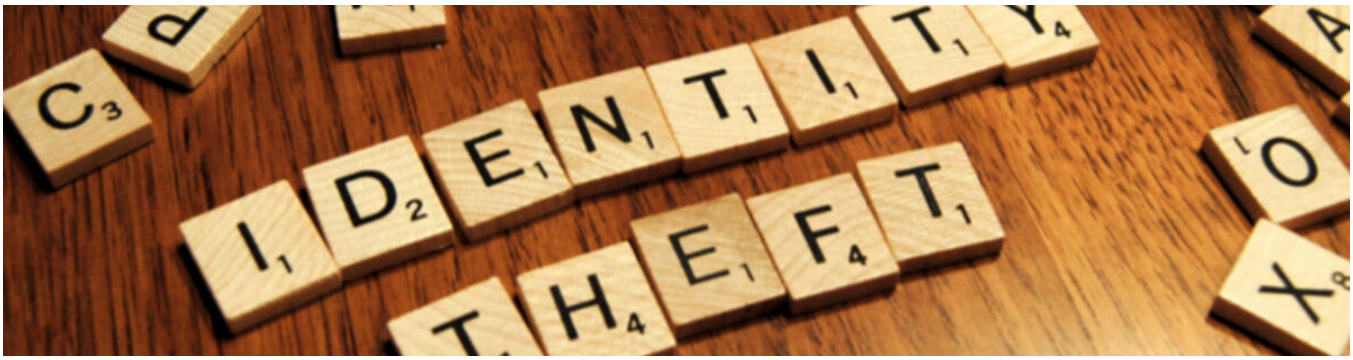
Identity Theft



It can start with a very official-looking email, a phone call from what appears to be an official number, lost or stolen wallets, or stolen mail. There are always new schemes being developed where people create notices through mail, email or even by phone that appear very official, but they are not. Phishing scams by email are becoming increasingly more sophisticated and are made to look like they are coming from an authentic source (the university, your financial institution, a personal contact). While more often than not, private sales of goods through email lists are legitimate, there is a potential for scamming you out of your money – never give or send cash/check without seeing and receiving the goods in question. In all instances, if you have questions or are concerned about a contact, please check with OISS.

When is it OK to Give Out My Personal Data?

Generally your bank, employer, the Internal Revenue Service (for tax purposes), and the Department of Motor Vehicles (for your license application) have a legitimate need to collect your personal information. Utility companies, cell phone providers, prospective landlords, and credit card companies (for your credit card applications) will also ask for your personal information such as a social security number (SSN). However, these entities understand identity theft issues and would never request your information in a way/ through a medium that would put you at risk. When it doubt, do not give out your personal information.

What Can You Do to Prevent Identity Theft?

- Ask OISS, your employer or school administrator before you give out personal information
- Keep personal data (bank account number, SSN, passport, etc) in a safe and secure place
- You have no obligation to respond immediately (to mail, email or phone calls) so disregard the request until you can talk to others to see if it is legitimate
- Know that immigration officials would never ask for a fee payment over the phone
- Most offices (Yale, banks, U.S. government) would never ask for your SSN, or personal passwords over email
- **Phone call scams:** If they insist on immediate action, ask for their name and phone number and say you will call them back in a few minutes. Then ask others (including OISS) if the situation sounds legitimate or not.

Understand and Report Identity Theft

- USA.gov - Prevent and Report Identity Theft [1]
- Yale Information Technology Services - Secure Computing [2]
- Federal Trade Commission - Identity Theft [3]
- **Report any issuance of immigration fraud to** safe@yale.edu [4] **and** OISS [5] **immediately.**

Digital Security **[6]**

There are no “magic bullets” to keep you and your information safe from scammers, malware, surveillance, and cyber criminals. A combination of tools and techniques [6], however, can drastically increase your Internet security and privacy.

Source URL:https://oiss.yale.edu/campus-community-life/for-students/safety-resources/scams-fraud/identity-theft

Links
[1] https://www.usa.gov/identity-theft [2] https://its.yale.edu/secure-computing [3] https://www.consumer.ftc.gov [4] mailto:safe@yale.edu [5] https://oiss.yale.edu/about/connect-with-oiss [6] https://cybersecurity.yale.edu/