Security

What we do to protect your personal information

At Snagajob, we work hard to keep your information safe. Internal procedures include:

- Regular risk and security assessments
- Methods to prevent and detect unauthorized access
- Testing of components by internal and third party experts
- Real-time alerting and on-call response to issues

We promise to:

- Keep your data safe and confidential
- Store your data encrypted
- Use industry-standard encryption protocols to protect all data in transit
- Protect our infrastructure and hold any providers we use to the highest expectations of physical access, control, and safety.

Your Part – What you should do

In General:

- Never share your login information with anyone to any website
- Never use the same password for all your online accounts (Netflix, Amazon, your email accounts, etc.) and try to change your passwords every 2-3 months
- Do not fill out social media quizzes that gather information about you (your birth month, your high school mascot, etc.) – you can't ever be 100% sure of where that data is going and who could use it to try and hack you.
- When looking at a web address, make sure "https://" is in the URL. This means that the website you're visiting is secure and that all communication between you and that website is encrypted.
- We recommend using a passphrase instead of a password. Learn more by clicking here – NIST Update: Passphrases In, Complex Passwords Out
- Never send personal information (Social Security Number, driver's license, DOB, etc.) or credit card information over email or text message
- Learn how to spot a phishing email – FTC's guide on phishing
    - If you get an email from a business, verify the sender by hovering over the email address

- Check for spelling mistakes
- Don't ever give up personal or company confidential information – most businesses will never ask for personal credentials via email
- Beware of urgent or threatening language in the subject line

Job Seekers – Common red flags when applying

It can sometimes be difficult to tell the difference between a real job posting and a scam posting. After all, scammers tend to advertise jobs openings inthe same places that legitimate employers do.

That's why we've put together some tips to help you keep your information safe during your job search. Watch out for these red flags and you will be able to tell the difference between a real job and a fake:

- **No work? No money.** Do not cash any checks or accept anymoney if you haven't done any work. Job scammers often say they will pay you in advance for miscellaneous items like office supplies or personal items. These checks are not real and they will bounce.If you are unsure, you can always go to your bank and have them confirm the authenticity of the check.
- **Share your info wisely.** Applying to many legitimate jobs online requires you to provide a lot of information, like your address or Social Security number.Just remember, never give out your information throughemail or over the phone. And always check to make sure the site you are using to apply is secure.
- **Stay organized.** Some scammers will post a job under a legitimate company name, but then contact youas a different, fake company in the hopes you won't rememberall of the jobs you've applied to. We recommend keeping a notebook or spreadsheet that lists each position and company you send an application to and don't respond to anyone unfamiliar.
- **Do your research.** If someone reaches out to you from a company you'venever heard of, do a quick internet search to check them out to see if others have been scammed by them. Also, keep an eye out for people who do not have a company domain name in their emailaddress, but instead use a free email service (e.g., XYZ@companyname.com vs. XYZ@gmail.com).
- **Be cautious with IM interviews.** If the employer does not want to meet you face-to-face (whether in person or over video) this is good sign that the job is a scam.In addition, they'll most likely hire you on the spot during the chat interview and ask for your bank account information. Never give this information out through an internet chat.
- **Trust your gut.** If it sounds too good to be true, it probably is. Pay attentionto the pay rate you are being offered and compare it to similarjobs in your area. If they offer to pay you $30 an hour to answer phones at home because their office is under construction, let this be a red flag.

What to do if you suspect you've been avictim of fraud

1. **Place an initial fraud alert** - Ask credit companiesto put a fraud alert on your credit report. This will make it difficult for anyone to access your account and lasts 90 days. More information canbe found here: FTC – Place a Fraud Alert
2. **Order a free credit report** - After you've placed an initial fraudalert, you will be entitled to a free credit report. More information: FTC – Order a Credit Report
3. **Create an identity theft report** - This report will help you deal with creditreporting companies, debt collectors and businesses. You can also use thereport to get fraudulent information removed from your credit report and can extend the fraud alert on your credit report. More information: FTC – Create an identity theft report
4. **File a complaint with the FTC** - This will help prevent anyone from openingaccounts in your name. More information: FTC – File a Complaint
5. **File a complaint with the Internet Crime Complaint Center** - a partnership between the FBI and national White CollarCrime

Center. More information: FBI/WCC – Internal Crime Complaint Center