A Message from Bristol-Myers Squibb Company

As a result of the increasing number of hiring scams, Bristol-Myers Squibb is providing this message as a form of guidance to those seeking employment with our company.

- BMS does not require advance payments from its applicants for any reason, including materials or software. If you receive this type of request, this is a scam and not a legitimate BMS position.

- File a report to the FBI Internet Crime Complaint Center (IC3) at http://www.ic3.gov/default.aspx or the FTC at https://www.ftccomplaintassistant.gov

- If you replied to a posting from a job website, contact the website to report the scam so that they can take action immediately.

- Notify BMS’s Customer Information Center at 800.332.2056 to report the scam.

The following information was created as part of a joint effort between the United States Secret Service, the Federal Bureau of Investigation, the Internet Crime Complaint Center (IC3) and the Financial Services Information Sharing and Analysis Center (FS-ISAC). Additional information was gathered at the CareerBuilder site.

Fight Online Fraud

Common Questions about “Work at Home” Scams

- What are Work at Home Scams?

While there are legitimate work-at-home jobs today, it is very important that a Job Seeker is able to identify the legitimate opportunities from work-at-home scams.

Work at Home scams are "positions" which claim that almost anyone can perform the job and earn lots of money from the comfort of home and without any advanced skill, knowledge, or training. They may sound like great opportunities for earning some extra cash, but in reality, falling for one of these scams only leaves the Job Seeker frustrated and with an empty wallet.

Whenever you use a job seeking web site you should exercise caution at all phases of your job search. For example, the "employer" may ask for a “required” upfront payment for instructions about the position, required software, or materials. Or the employer may require a "subscription fee" or initial start up fee be paid before they send any information to the Job Seeker. Once the job seeker makes a payment, the job seeker is told that the materials and information will be mailed or emailed to them within several business days.

If the job seeker even receives the materials/software needed to start their new "job", the materials are usually of very poor quality and the information provided is minimal. Typically, the job seeker is given instructions to assemble the products or transcribe data. However, when the task has been
completed, the fraudulent employer immediately rejects the work claiming that it didn’t meet the required standards or did not pass their quality control test. Often these employers require a repurchase for another kit/software at a "discounted rate" to receive another payment from the Job Seeker. The fact is that all work submitted to the employer will be rejected as it will never "meet quality standards." Remember this; **the job seeker is left with less money and will never be paid by the "employer."**

In some cases, the job seeker will not receive any materials to start employment. Attempts to contact the employer will be unsuccessful, due to the lack of valid contact information provided for the company. Again, the job seeker is left without any working materials and may be further in debt.

**Signs of a Work at Home Scam;**

- Company initiates contact with you from a generic or free online web email address.
- Company information cannot be verified.
- **Company requires advance payment for materials or software.** (Some legitimate companies will require a fee, however you should be very careful and fully investigate the opportunity)
- Company is located overseas.
- Misspelled words, grammatical errors appear in the job offer and corresponding emails.
- Job description promises high income for very little time and effort; no experience necessary.
- Employment starts without a face to face interview.
- Company is requesting bank account information or for the jobseeker to use personal bank account.
- **If the job sounds "too good to be true", it probably is.**

**Protecting yourself when job seeking;**

- Research the company that is offering the position. Check the internet and Better Business Bureau for the company name, phone number, and location. If you are suspicious of the posting and have a phone number available, place a call to the company and inquire about the job details.

- Look for resources on line which provide you with helpful websites to enhance your job search and research if there is negative feedback on a company.

- **Think before you apply:** If a company is offering a high wage or salary for very few hours of minimal work, it would not be ideal to forward them your personal information. It’s best to investigate before sending any of your information to a potential employer.

- **Seek local employment:** If a company states to be located overseas, first research the company. Next, contact the company directly, inquiring about the opportunity being offered. You may also submit a ticket to our Trust and Site Security Team to verify the legitimacy of a company or opportunity.

- **Do not cash/wire/ship any checks or products:** Companies will never ask you, for any reason, to set up a bank account, to deposit checks, or to accept direct fund transfers into your own
account and then wire them to another source. If you receive an email requesting you to do so, cease communication with the company, and Bristol Myers Squibb immediately.

• **Ask questions:**

Ask specific questions to the employer that is offering the position. The posting should provide enough information about the position, however if a description seems vague, report the job to the site you are on. Look for "Report this Job" forms for whatever site you may be using to notify them of questionable jobs posted on their website or forward any suspicious job offers you received in email to them.

• **Never provide sensitive personal information during the initial application process.**

Be extremely careful providing information such as your Social Security number, Drivers License number, Date of Birth, or other sensitive information that might make it easy for a fraudster to use that information to steal your identity. We recommend that you never place this type of information on your resume. However, please keep in mind that most companies will require your social security number when filling out an actual application. If you are asked to fill out an application online, on that employer’s website, you can check to see if that page is secure (the address bar should read "https:"). Pending that outcome, it is entirely up to your discretion as to whether you would like to apply online or not. You may want to contact the company directly to find out if there are other methods of application.

• **Below are some helpful questions to ask the employer:**
  - What specific duties will I have to perform on a daily basis?
  - What are the normal business hours?
  - Does your company have a website or additional information about this position?
  - Is your company registered with the Better Business Bureau?
  - Will I be paid salary or commission?
  - Who will be distributing my income?

**Protect Yourself:**


• (For international companies) before providing personal or account information and/or agreeing to work for them. In addition, [https://trustedsource.org/sources/index.pl](https://trustedsource.org/sources/index.pl) can help you identify companies that may be maliciously sending spam based on the volume of email sent from their Internet Protocol (IP) addresses.

• See also the FTC’s recommendations at [https://www.consumer.ftc.gov/scam-alerts](https://www.consumer.ftc.gov/scam-alerts)

• Be cautious about any opportunities offering the chance to work from home with very little work or prior experience. **Remember: if it looks too good to be true, it usually is.**

• Never pay for the privilege of working for an employer. Be suspicious of opportunities that require you to pay for things up front, such as supplies and other materials.

• Never give your bank account details to anyone unless you know and trust them.
• If you think you may be a victim of one of these scams, contact your financial institution immediately. Report any suspicious work-from-home offers or activities to the Internet Crime Complaint Center (IC3) at [http://www.ic3.gov/default.aspx](http://www.ic3.gov/default.aspx)

For more information, visit:
- [https://www.consumer.ftc.gov/features/feature-0038-onguardonline](https://www.consumer.ftc.gov/features/feature-0038-onguardonline) (OnGuardOnline) Sponsored by the FTC, this site provides practical tips from the federal government and the technology industry to help you be on guard against Internet fraud, secure your computer, and protect your personal information.

Additional Resources for Fraud Security:


**What do I do if I am the victim of a Work at Home Scam?**

- If you have paid in advance for materials, software, or fees in conjunction with a work at home position and attempts to contact the employer are unsuccessful, contact your bank or credit card company immediately to attempt to stop or reverse charges.
- If you wired money, contact your bank immediately and request to stop the wire. Advise the bank of your situation.
- File a report to the FBI Internet Crime Complaint Center (IC3) at [http://www.ic3.gov/default.aspx](http://www.ic3.gov/default.aspx) or the FTC at [https://www.ftccomplaintassistant.gov](https://www.ftccomplaintassistant.gov)
- If you replied to a posting from a job website, contact them to so that they can take action immediately.

Lastly, be aware that many emails claim that the hiring company is advertised on a particular job website; **however a great majority of these emails are spoofed**, and not derived from the actual job website database.