SECURITY TIPS FOR SAFE ONLINE JOB HUNTING

NATIONAL CYBERSECURITY ALLIANCE

IN COLLABORATION WITH

Looking for a new job can be a daunting project, and frequently involves the exchange of personal information with complete strangers--which is why job seekers are an enticing target for cyber criminals. As you look for a new job, be extra vigilant so your application materials and personal information don't end up in the wrong hands.

TIPS TO PROTECT YOURSELF

DO YOUR RESEARCH

- Conduct a web search of the hiring company using the company name only. Results that return multiple websites for the same company (abccompany.com and abccompanyllc.com) may indicate fraudulent job listings.
- Check for spoofed websites. Scammers will often spoof legitimate websites with the exception of small discrepancies in order to deceive victims.
- If the hiring company is well known and has a website, contact the company to confirm the legitimacy of the job listing. It is likely the legit company has received other calls and can confirm a scam listing.

DON'T PAY TO PLAY

- Never send money to someone you meet online, especially by wire transfer, prepaid cards, or money transfer apps.
- If you receive any paper checks with instructions to purchase items or transfer money, contact the financial institution on the check to ensure the availability of funds.
- Never provide credit card information to an employer.
- Never provide bank account information to employers without verifying their identity.

Fake Job or Hiring Scams occur when criminal actors deceive victims into believing they have a job or a potential job. Criminals leverage their position as "employers" to persuade victims to provide them with personally identifiable information (PII) or to send them money.

FBI Public Service Announcement I-012120-PSA

PAUSE BEFORE SUPPLYING SENSITIVE INFO

- Legitimate companies will ask for personally identifiable information (PII), such as social security number and bank account information for payroll purposes, AFTER hiring employees.
- Before entering PII online, make sure the website is secure by looking at the address bar. The address should begin with "https://", not "http://".
- *However:* criminals can also use https:// to give victims a false sense of security. A decision to proceed should not be based solely upon the use of "https://".

SECURITY TIPS FOR SAFE ONLINE JOB HUNTING

NATIONAL CYBERSECURITY ALLIANCE

IN COLLABORATION WITH

REDO YOUR RESUME

- Consider removing sensitive information from your resume, such as your home address. You can also use a forwarding phone number instead of your actual phone number.

POSTS ON JOB BOARDS AREN'T ALWAYS LEGITIMATE

- Websites that catalog job openings can't easily verify the legitimacy of every single opportunity. If you see a job on a job board, go directly to the company's website to see if the job is also posted in their careers section. If it isn't, this is a good sign the post is not legitimate.

Get savvy about WiFi hotspots

- When applying for jobs, try to use a secure network--not public wifi. For instance, use a virtual private network (VPN) or your phone as a personal hotspot to surf more securely.

Make your passphrase a sentence

- For most jobs you have to create an online job profile with the company, which means establishing a unique username and passphrase for each. A strong passphrase is a sentence that is at least 12 characters long. Focus on positive sentences or phrases that you like to think about and are easy to remember (for example, "I love country music.").
- Enable 2-factor authentication on all accounts that offer it for an extra layer of protection.

Think Before You Click

- Do not click on unsolicited links in emails, social media messages, text messages, etc. Confirm any links, especially those collecting sensitive information, were intentionally sent by the hiring company.
- Resist the urge to act quickly, especially when receiving and sending money.

Be wary of those posing as recruiters.

- Has a recruiter emailed or messaged you directly? If their email is from a generic domain (e.g., not from a corporate domain), ask them to email you from their corporate email address. Check to ensure the corporate email matches the website. Some scammers will spoof a legitimate email with minor variations to fool victims.
- Do your research on the recruiter. Check to see how many followers they have, make sure they have a complete and professional profile, and do an internet search of their photo to see if it is used on other accounts associated with different names.

SECURITY TIPS FOR SAFE ONLINE JOB HUNTING

NATIONAL CYBERSECURITY ALLIANCE

IN COLLABORATION WITH

LEARN MORE

- FBI IC3 Job Hunting Scams Public Service Announcement: https://www.ic3.gov/media/2020/200121.aspx
- Federal Trade Commission Job Scams Resource: https://www.consumer.ftc.gov/articles/0243-job-scams
- If you are a victim of a hiring scam, the FBI recommends taking the following actions:
  - Report the activity to the Internet Crime Complaint Center at www.ic3.gov or your local FBI field office, which can be found online at www.fbi.gov/contact-us/field-offices.

NATIONAL CYBERSECURITY ALLIANCE

The National Cyber Security Alliance (NCSA) builds strong public/private partnerships to create and implement broad-reaching education and awareness efforts to empower users at home, work and school with the information they need to keep themselves, their organizations, their systems and their sensitive information safe and secure online and encourage a culture of cybersecurity. www.staysafeonline.org

The mission of the Internet Crime Complaint Center (IC3) is to provide the public with a reliable and convenient reporting mechanism to submit information to the Federal Bureau of Investigation concerning suspected Internet-facilitated criminal activity and to develop effective alliances with law enforcement and industry partners. Information is analyzed and disseminated for investigative and intelligence purposes to law enforcement and for public awareness. Learn more at: www.ic3.gov