AMINA
CORP.CA

Privacy for Responding to Online Ads

If you're wondering how to protect yourself before answering online ads that ask for personal information, follow these simple tips to help guard against identity theft.

1. Before responding to any ad online, whether online or by email, verify that the opportunity is legitimate and not merely a ploy to obtain personal information. Research the person/company asking for the details to be sure they're for real. Do some research and contact the company directly. If the offer sounds too good to be true, it probably is. If you're not sure, call your local police and ask if they've heard of offers like this one that turn out to be cyber frauds.
2. Create and use a separate email address and account for online job-hunting, dating and shopping activities. Using your usual email account allows the other party to search the Internet for that email address and discover a wealth of information about you.
3. Review the privacy settings on your social networking accounts to prevent others from seeing photos and comments, and from drawing conclusions about you based on what they see.
4. Be wary of anyone who offers you money up front. Some online scams (like the house rental or "secret shopper" ruses) involve sending a cheque to the victim with instructions to keep a portion of the funds, and send a portion to someone else, often in another country.
5. Employers in most jurisdictions aren't allowed to ask for certain information as part of the hiring process; don't volunteer it when you post a resume or apply for a position — especially not online, in emails, or by fax because you really can't know where your information is going. This isn't the time to reveal your marital status, birth date, social insurance number, social security number, credit card information, passport information, or details about your spouse or children.
6. Beware of anyone that asks for money or for a credit or background check before they'll process your application. Legitimate employers and recruiters don't ask for that information at the outset.
7. Be wary of anyone who asks for your online identity, passwords or logon credentials. Interviews are notorious for being power imbalances: You want the job, so you feel powerless to refuse the recruiter or employer's request. The law might be on your side, though: Many jurisdictions have outlawed the practice of asking for access to social network profiles, and many employment or human rights laws condemn the practice.
8. Avoid posting your resume online. It's too easy to match the details in a resume with other information on the Internet and derive a comprehensive profile of you, your activities, location, associations and other details that would be useful to use against you.
9. Edit your resume before sending it out, to be certain that the details about your expertise and accomplishments don't jeopardize the privacy and security of projects you've worked on. Identifying the technology, platform, or technical details along with the employer/client and project could be enough for someone with questionable motives to defeat system safeguards.
10. Personal information is often embedded in documents as they're created. Check the document properties, and remove that metadata from your resume and other documents you send out.
11. Encrypt documents before sending them out to keep the contents secure from prying eyes.
12. Password protect documents so they're harder to change or copy without your consent.

• Data Protection • Privacy • Information Risk Management •

• pragmatic • trustworthy • reliable • secure • dedicated • ethical •

Global Headquarters
Suite 330, Unit 440
10816 Macleod Trail SE
Calgary AB Canada T2J 5N8
Telephone +1.403.254.4376
www.AMINAcorp.ca

For more information about practical ways to protect you privacy and reduce risk, visit www.AMINAcorp.ca or contact us by email at info@AMINAcorp.ca or by phone at +1.403.254.4376 for a private conversation.