

As society begins to reopen, scammers aren't keeping 6 feet away from your personal information.

Watch out for these trending scams as the country reopens:

### **Account Takeovers**

Shorter hours and percentage-capacity rules mean many consumers are still shopping remotely. This leads to an increase in online retail scams, like [account takeovers](#), where scammers hack a company's database to break into a customer's account. Using the customer's remembered payment information, the scammer goes on to place large orders to their own address — all on the client's dime.

**Protect yourself:** Account takeovers are most commonly pulled off on dormant accounts. Outsmart the scammers by checking your retail accounts for sudden orders, or deleting remembered information on accounts you rarely use.

### **Job Scams**

The [FBI](#) is warning against a surge in scams in which cybercriminals pose as employers by spoofing websites and posting bogus job openings on online boards. Sometimes, they'll even conduct "interviews" with applicants. The scammers ask for personal information, and may demand payment before the "application" can be processed. Of course, there is no job waiting for the applicant, their information is in danger of being abused and they'll never see that money again.

**Protect yourself:** Beware of outrageous job claims that promise big money for little work. Never share sensitive information online with an unverified source. Finally, before agreeing to an interview, research an alleged company on the [BBB website](#).

### **The Contact Tracer Scam**

The [FTC](#) is warning of a new ruse in which scammers impersonate a COVID-19 contact tracer and reach out to people via phone call or text message. They'll ask for the victim's personal information, including their Social Security number, claiming they need it for their work. They'll use this information to pull off identity theft or hack the victim's accounts. Sometimes, the scammer will ask the victim to click on an embedded link, which will grant them access to the victim's phone.

**Protect yourself:** Contact tracers will always identify themselves and their department. If a contact tracer reaches out to you, verify authenticity by researching this information. Most importantly, they have no need for your Social Security number nor will they ask for it.

Stay aware and stay safe!