HP Fraud Alert: Protecting Yourself from Scams

This document is for all HP products.

Telephone technical support scams are an ongoing threat to technology companies such as HP and our customers. Scammers might call you on the phone and pose as representatives from HP technical or customer support. In some cases, scammers mask their originating phone number (Caller ID spoofing) so the calls appear to be from a genuine HP contact number.
The scammers attempt to gain your trust, and they might employ one or more of the following tactics:

- Try to convince you that your device requires urgent technical support, and then request payment information (such as credit card, debit card, or online gift card) to bill you for phony services.
- Request you to call them back at another time to "complete" a fraudulent technical support case and potentially further the scam.
- Request remote access to your device, or try to convince you to install software that enables remote access to the device.
- Try to trick you into installing malicious software including malware, viruses, or spyware that could capture or jeopardize the security of your personal information, such as online user names or passwords.
- Request you to provide confidential information such as user IDs, passwords, customer support case numbers, or account history.
- Become aggressive and demand that you follow their instructions.

Protect yourself from telephone tech support scammers

What to do after you have been contacted by a scammer

Learn more about tech support scams

What HP is doing about tech support scams