Avoid Malware Infections

Trust is Tops

Only Use Trusted Apps or Software: Only download apps directly from trusted app stores (iTunes, Google Play) or software sites (CNet). Be wary of unfamiliar apps or software or "look-alikes". Check ratings and reviews in the app store; if a major retailer only has one review or a low rating, it might be a copycat and you should avoid the app.

Don't Trust Every Download or Search Result: Just because you get a lot of results a search doesn't mean you should download spreadsheets or documents to view them. Documents and spreadsheets are notorious for hosting malware with embedded macros. If you frequent forums or communities of interest, ask what software others have used and if they've had problems with it.

Beware of "Extras" When Installing Software: Legitimate software or browser add-ins can be accompanied by unasked for software; remember that every new app, software, or browser toolbar can be a new entry point for hackers, so uncheck extra software options unless you really need them.

Don't Click That

Beware of Unexpected Emails: Scammers are using fake package tracking emails for online retailer purchases. When someone clicks the tracking link, they infect their computer with ransomware which encrypts their computer and requires them to pay a ransom to regain access.

Double-Check Links: Links in emails and social media posts require caution. Don't click the links without hovering over the URL and making sure it's taking you to a legitimate website before clicking.

IBM Security

Avoid Identity Theft

Be Stingy With Your Data

Don't Save Your Info: Never save credit card information in retail or bill payment sites, or even in the web browser itself. Internet browsers are among some of the most successful attack vectors that hackers can use.

Be Smart About Your Passwords

Use a Special Shopping Email Address and Password: Have a separate email address just for shopping websites, and make unique passwords for each online store. Never reuse the same password on different websites. Instead, create a unique passphrase for each site or use a password wallet to create unique passwords and store them.

Get Creative With Password Reset Questions: Opt for the password reset question that can't be figured out from social media. Pick something that can be an opinion question (favorite dessert, band, etc.), make up answers only you know, or use a password wallet to create a unique answer to the question and store those answers securely.

Control Credit Card Usage

Opt for Credit Over Debit Cards: Credit cards offer consumers more protections if the card is compromised, and won't impact your checking account if there's an issue. Consider a one-time use credit card when buying from a non-trusted or entirely new retailer. Be sure to check accounts frequently during the holiday season for unusual activity.

If you're concerned: Visit any of the three credit bureaus, Equifax, Experian, or TransUnion, for more information or to place a fraud alert or freeze on your credit report.