That Unexpected Package Could Be a Scam

Imagine you receive a package from an unknown sender containing items you didn't order. While this might seem like a welcome retail mistake, it could actually signal a more nefarious situation. The sender may intend to make you appear as a verified buyer and write fake reviews in your name to fraudulently boost online ratings and sales numbers. This is called a brushing scam.

Why **Brushing Scams** Are Concerning

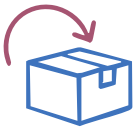
In recent years, perpetrators have enhanced their brushing tactics to include ***quishing*** or "QR code phishing." Phishing usually involves a scam email or text message to trick you into revealing personal details; quishing uses similar methods through QR codes.

In a quishing scam, the sender encourages you to scan a code with your smartphone, which may lead you to a fake website intended to steal your personal information.

How to Avoid **Brushing Scams**

If you find an unexpected package on your doorstep and believe it may be part of a brushing scam, consider the following steps:

Decline to pay for the merchandise if asked to do so.



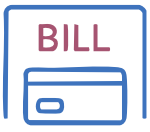
Return the package to its sender if it's unopened and includes a return address.

Throw away the package if its materials appear safe for typical disposal.

Notify authorities if the package contains organic materials (e.g., seeds, plants or food) or an unknown substance.

File a fraud report with the retailer (e.g., Amazon or eBay) and ask them to delete any fake reviews made under your name.

Change your account passwords.



Monitor your credit card bills, bank accounts and credit report for fraudulent activity.

Learn More

For more information on possible scams and cyber safety, contact us today.