BRANDPROTECT EXECUTIVE THREAT BRIEF

brandprotect™

October 2017 | Briefing 35

BUYING AND SELLING ONLINE – IS IT TOO GOOD TO BE TRUE?

These days, people can buy and sell almost anything online. Unfortunately, cybercriminals have taken advantage of internet anonymity to scam buyers and sellers.

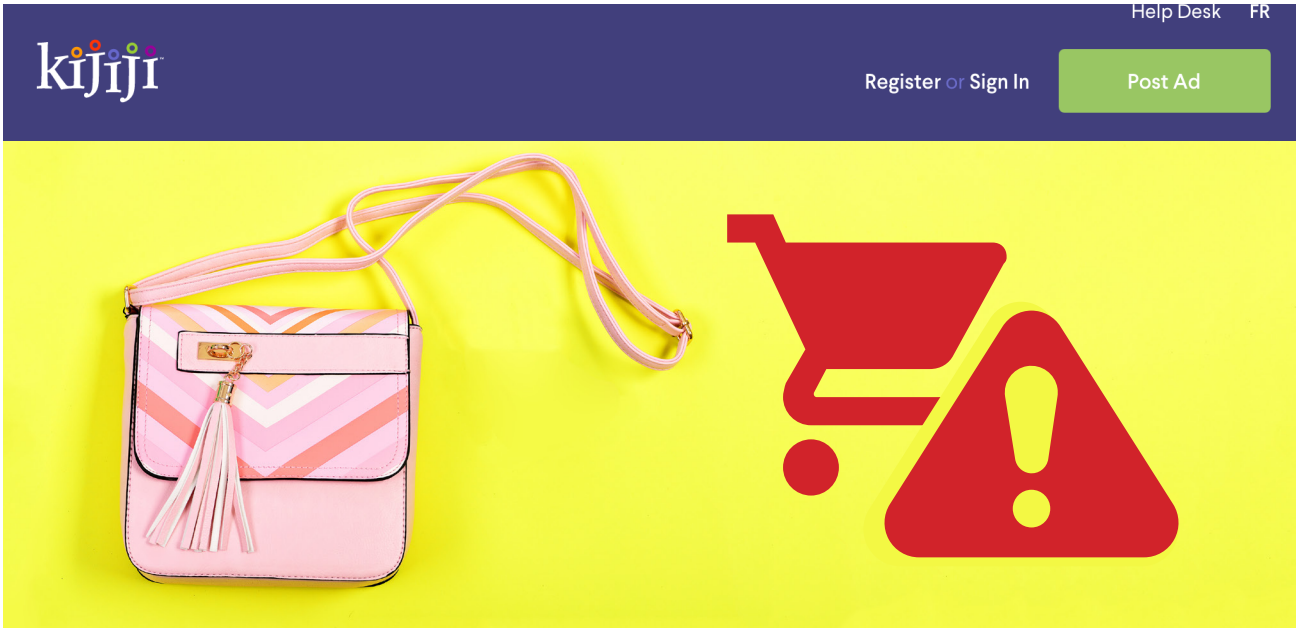
Online sales in the United States are expected to reach $523 BILLION by 2020, Forrester Research Inc. says.

Seller Beware!

Kijiji PayPal Scam: You place an ad on Kijiji in hopes of selling an item. The potential buyer advises you that they live far away and asks for the item shipped to them but are willing to pay higher value than the asking price to cover shipping costs. The buyer and you agree to set a price and the item to be purchased through PayPal. What happens next? There are several possibilities on how the scam may unfold:

1. **YOU DON'T HAVE A PAYPAL ACCOUNT.** You'll need to set one up, right? No problem! The buyer sends you an email with a link to help you set it up. But the link takes you to a fake PayPal website and your information could potentially be used to commit fraud or even identity theft.

   Be wary: Always go directly to PayPal.com if you need to create an account.

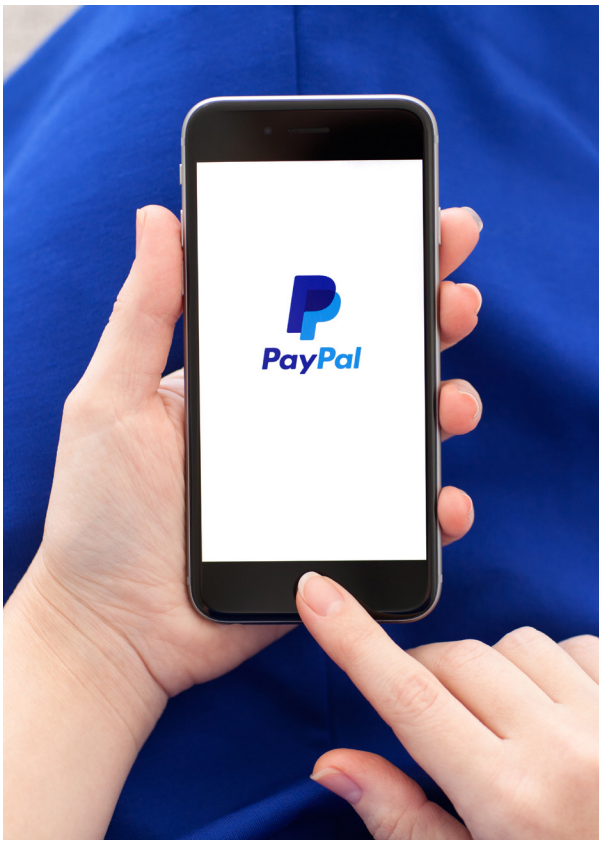


2. **THE BUYER PAYS THROUGH PAYPAL AND YOU SHIP THE ITEM:** Ideally the transaction should be completed at this point or so you think. The problem is the buyer used someone else's PayPal account and now you might need to return the money.

   What happens next? You'll need to file a complaint to PayPal and open an investigation with your local police department.

3. **YOU RECEIVE AN EMAIL FROM "PAYPAL"** advising you the buyer sent the money but in order to complete the transaction you need to send the shipping fee. You pay the fee and you never received the payment. Why? Because paypal@online.net was not a legitimate PayPal email address and you were scammed.

   How did THAT happen? First of all, if a buyer agrees to pay extra money to cover shipping costs always be alert as it is likely a scam. Second, before sending the item always check your PayPal account and make sure you have received the money (by going directly to your account and not through a link in an email). Finally, check the sender's email address and confirm it with the one on the website before taking any action, even replying to an email can give the scammer enough access to your information.



KEEPING YOUR TRANSACTIONS SAFE

Thinking about making online purchases? Here's some tips that can help ensure you have a safe experience:

- **Check the sellers' reviews:** What previous customers have to say about a company says a lot about them. Do they have many poor reviews? Are people saying only negative comments? If so, think twice before going further with the transaction.

- **Research the website:** Make sure you're shopping at a secure website, look for a URL starting with 'https' and a closed lock symbol. Check if the website has return or refund policies and if they provide support in case something goes wrong.

- **Avoid using public Wi-Fi when buying online:** Protect your confidential information by using a secure network. Using a public Wi-Fi leaves you vulnerable to hackers lurking and stealing your data.

- **Use your credit card:** Avoid paying with your debit card, so if there's any problem you can't solve with the seller or shopping site, you can contact your credit card company and have them return your money.

- **Don't click on email links:** Don't fall for phishing emails requesting you to update your account information or passwords. Even if the email comes from a familiar address it may be a spoofed email address. Call the company to verify the information and use the contact us info provided on their website.

- **Track your purchase:** Keep a close eye on the purchases you make by monitoring your bank account balance and immediately report any unusual charges.

- **Protect your mobile phone:** Smartphones can be potential targets. Keep your data safe by setting your device to automatically lock when it's not in use. Also make sure you are always downloading Apps from the official App stores (i.e. Google Play, ITunes etc.)

While online shopping is increasingly popular, cyber security has become a tremendous concern. Like with any website always protect yourself when buying or selling online and follow your instincts, if something seems "phishy", it's probably a scam.

brandprotect™

www.brandprotect.com
sales@brandprotect.com | 1.866.721.3725

For enterprises concerned about their business exposure to increasing online risk, BrandProtect™ provides a complete suite of world class Internet threat detection services to monitor the entire social Internet spectrum and mitigate business risk arising from fraudulent or unauthorized online activity. BrandProtect helps security, risk management, and marketing organizations at leading financial services institutions, large-scale retailers, insurance providers, telecoms, pharmaceuticals and more, protect their brand value and business bottom line.