Talk Nerdy To Me



Romance Scams Ahead of Valentine's Day



Last year, scammers took in a record amount of cash in romance scams, according to the Federal Trade Commission. In a new report, the FTC says consumers lost more than \$300 million to romance scams in 2020 -- a 50% increase from the previous year.

Now during the pandemic and ahead of Valentine's Day, the FTC is warning about scammers creating fake profiles and taking advantage of the pandemic and the economic crisis.

"We have had people report -- hundreds of people report -- that these scammers were sending them fraudulently obtained unemployment benefits," said Monica Vaca, FTC associate director for the division of consumer response and operations.

The biggest age group that scammers have targeted? People who are 20-29 years old.

To avoid falling victim to a romance scam, the FTC advises people to use this checklist to determine if you're being scammed.

1. Scammers make excuses to not meet in person

Vaca said that this has been easy during the pandemic. "There are some people that have even said things like, 'I just tested positive for COVID... I can't meet up with you today."

If the person you're speaking with repeatedly rejects invitations to meet up in person, Vaca said you're likely being scammed.

2. Never send money

To avoid Fraud, the FTC advises to never send money or gifts to someone you haven't met yet. Instead, take it slowly, ask questions and look for consistent answers.

3. Do a reverse-image search on the person's profile photos

If the picture is associated with another name or with details that don't match up, it's likely that the relationship you've forged with the person you met online is a scam.



5 Tips To avoid Being Scammed When Using A Payment App



Many Americans are more likely to send money to friends and family through a payment app on their smartphone than write a check these days. It's convenient, easy to use and, for some, a contactless transaction that may reduce health and safety concerns during the COVID-19 pandemic. Yet there's another major factor to consider: fraud.

"Consumer complaints are rising steeply within the mobile app payment industry," said Kia McCallister-Young, director of America Saves, an initiative of the Consumer Federation of America. Fraud rates among mobile payment apps are three to four times higher than traditional payment methods, according to the CFA, and are being exploited by scammers.

"People of color and low-income earners are targeted by scammers at higher rates than other consumer demographics," McCallister-Young added. The CFA found that among Black and Latino consumers, two in five have been targeted by a scam and one in five have lost money due to a scam.

Mobile payment apps can be very attractive to scammers, experts say, since you generally don't get the same fraud protection as you do with debit and credit cards. Scammers may link a stolen credit card to a payment app to make a purchase, set up transactions and cancel them before they go through or send an email saying you were overpaid for an item and need to send the money back. And with an app, money transfers happen so quickly that it can make it difficult to detect fraudulent payments.

With mobile payment apps, "the beauty of it is that it's instant," said Ted Rossman, senior industry analyst at Bankrate.com. "The problem is that it's very hard to get the money back. You definitely need to make sure that you're sending it to the person you want to send it to."

The type of online payment system you use may also have an impact on whether you're more or less likely to lose money if you are scammed.

According to a 2021 report from the Better Business Bureau, the median dollar loss for online purchase scams was \$90 for PayPal, which is much lower than median losses reported for Zelle, Venmo, Apple Pay, Google Pay and Cash App. PayPal can be linked to bank accounts or credit cards. Zelle allows bank-tobank transfers, but you can't link it to your credit card. The differences in the way money is transferred can result in different payment protections.

No matter which mobile payment app you choose, the BBB and other experts recommend these five tips to avoid being scammed:

1. Transfer money only to people you know and make sure you have the correct phone number or email for that person when making the transfer.

2. Enable security features like multi-factor authentication on the app and your smartphone that may require a PIN, fingerprint or face recognition.

3. Keep your smartphone secure with a strong password, biometric features or two-factor authentication.

4. Link your mobile payment app to a credit card rather than a bank account or debit card.

5. And always check that the money transfer has been completed.

Source: https://www.cnbc.com/2022/01/25/5-tips-to-avoid-being-scammed-when-using-a-paymentapp.html

Our CEO Is A Published Author



Stay one step ahead of cyber criminals to protect your business, your customers, and your money!

In Jason's first published book, he talks about why cybercrime today cannot be ignored and why your network and data are cyber criminals' #1 target!

Learn all the ways to protect yourself and your data. Contact us today for your copy of *Inside The Hacker Mind.*



Happy Birthday Jason!



Wishing a Happy Valentine's Day <u>AND</u> a Happy Birthday to our fearless leader, Jason Horne.

Hope you have a wonderful day with lots of ice fishing!



February 2022

Grabbing The Bull By The Hornes - Preferred IT CEO, Jason Horne, Is Gaining Ground Fast

Check out Preferred IT Group's CEO, Jason Horne in MSP Success Magazine!

"So, in the sports bar that night, where patrons sampled cold beer and cheered on the Cubs and Komets, a vision for what would become Preferred IT emerged."



FUN FACT!





CONTACT US



 Fort Wayne
 W

 260.440.7377
 5

 Columbia City
 In

 260.213.4266
 3

Warsaw 574.306.4288 Indianapolis 317.426.8180



www.preferreditgroup.com



6333 Constitution Drive Fort Wayne, IN 46804

Subscribe to our blog and follow us on social media.

