Black Friday bargains or fraud traps: The risks of tap and go payments

Global contactless purchases are expected to more than quadruple between now and 2027. This significant growth will mainly be driven by payment-enabled mobile devices, such as smartphones and smartwatches.

Photo by energepic.com via www.pexels.com

“As we approach 2024, it is clear that contactless payments are more than a trend; it has staying power,” says Anna Collard, SVP content strategy and evangelist at KnowBe4 Africa. However, while the convenience of not needing to carry a wallet is undeniable, consumers should know the specific risks associated with contactless payments.

“Contactless payments have soared in popularity, transforming the way we pay for goods and services. With the tap of a card or a smartphone, consumers can complete transactions quickly and effortlessly,” says Collard. Whether it is grabbing a cup of coffee, purchasing groceries, or filling up your car with fuel, contactless payments have become an integral part of our daily lives.

How secure is this type of payment?

“Apple Pay and Google Pay are relatively secure contactless payments using their own combinations of passcodes, encryption, fingerprint- or facial-recognition technology,” explains Collard. “They have invested into ensuring you can protect your device and your accounts as effectively as possible. However, if you break the chain—use third-party apps, click on phishing messages, fall for scams—then these protections fall away and your device becomes vulnerable.”

Losing your phone or having someone get hold of your passcode is another major worry. In these situations, dishonest people can exploit your device to make unauthorised contactless payments. Staying alert and taking measures to safeguard your personal information is essential.

“Let me give you an example. You receive a text message that looks like it is from Apple pay or other mobile payment app. The message claims there is an issue with your account and asks you to confirm your login details by clicking on a link. The catch is, it is all a scam. When you enter your information, the fraudsters get access to your account. They could then make unauthorised transactions against your credit card, and making it incredibly difficult for you to get your money back.”

While smartphones and smartwatches are widely associated with contactless payments, tap-and-go technology is also available for traditional bank cards. However, using bank cards for tap-and-pay transactions poses its own set of risks.

“Fraudsters may attempt to skim or clone your bank card to gain access to your funds. Skimming happens when they use sneaky devices on real payment terminals to steal your card information. Cloning involves making fake cards with all your card details,” explains Collard. “When you are shopping at speed to catch the best Black November deals, you are distracted, which means it is easy for you not to see a skimming device and just tap your card.”

What you can do

To minimise the risks associated with contactless payments, follow these practical tips:

- **Set a strong passcode**: Choose a unique and strong passcode for your phone or smartwatch. Do not use readily apparent passcodes.

  Protect your Apple ID or other mobile payment apps IDs. Use two-factor authentication and never share your ID password or verification codes with anyone. Apple, Google or your banks would never ask for this information via text, email or the phone.

- **Enable biometric authentication**: Take advantage of features like facial recognition or fingerprint scanning to add an extra layer of security to your device. This way, only you can unlock it.

- **Keep your devices nearby**: Make sure to have your phone or smartwatch with you at all times and avoid leaving them unattended. Be cautious when lending them to others.

- **Regularly monitor transactions**: Stay vigilant by regularly reviewing your bank statements. If you notice any suspicious transactions, report them to your bank.

- **Change tap-and-go limits**: Change the tap-and-go limit on your card. You can easily do this in your banking app. By requiring a PIN for higher amounts, you add another layer of security to protect your funds.

- **Be cautious with your card**: Always keep your bank card in a secure place, such as a wallet or a cardholder. Avoid sharing your PIN with anyone.

“Tap-and-go payments are incredibly convenient, but it is important for consumers to understand the potential risks

involved," Collard concludes.

"By understanding the security measures in place, being cautious with personal information, and following practical tips for protection, you can safely enjoy the ease of contactless payments during Black Friday shopping without worrying about falling victim to fraud."