How to avoid online ticket fraud

There is no doubt that South Africans are excited to head back to stadiums to watch sport and to watch their favourite musicians. This can be seen in the almost immediate sell out of the Springboks versus Ireland test matches and the return of a number of international music acts like James Blunt, Take That, Green Day and The Offspring.

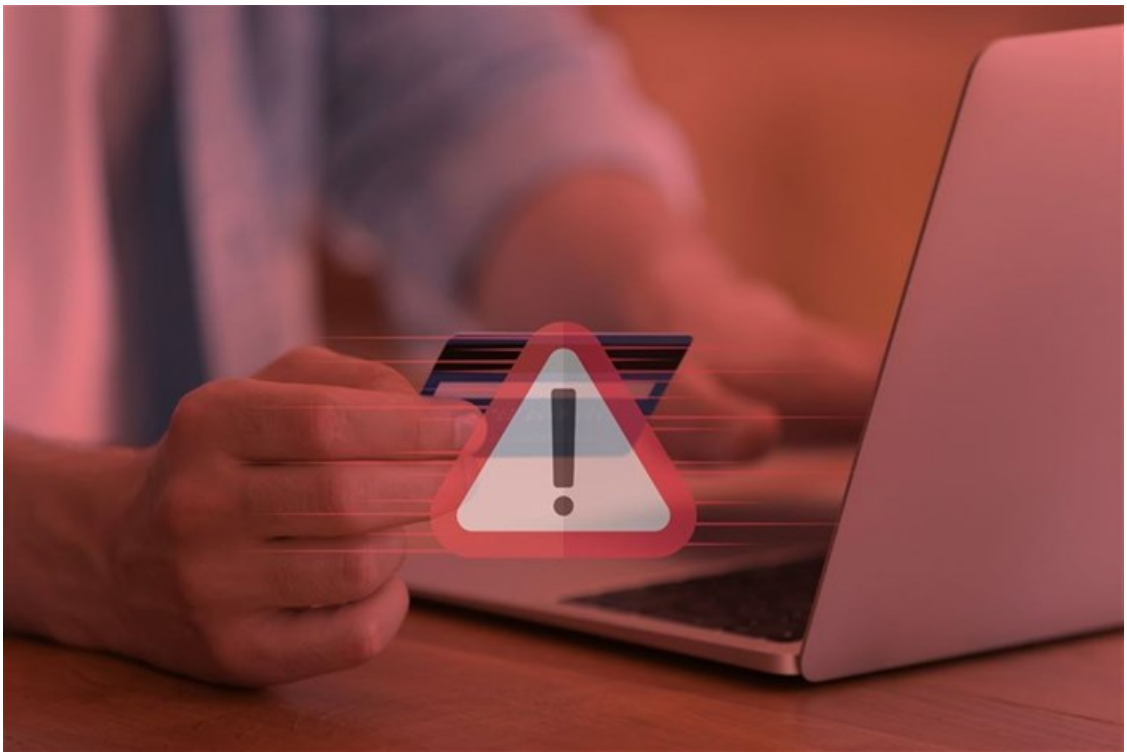

Image supplied

To secure a seat at one of these thrilling events, South Africans have hopped online to purchase their tickets. And as is the case with anything that involves a digital interaction and transaction, consumers are exposed to cyber risks. These can include phishing, malware and fake websites.

“There’s often a lot of excitement that comes with booking for a live event and this can lead to consumers being a little more relaxed about their online safety,” says Emmanuel Tzingakis, technical lead for sub-Saharan Africa at Trend Micro.

“Consumers need to be extra careful when it comes to booking for major concerts or sports matches, because there’s no doubt that cybercriminals will be looking for an opportunity to prey on unsuspecting victims.”

To help consumers protect themselves from cybercriminals and online ticket fraud, Tzingakis shares his top tips on how to spot a scam and stay safe.

1. Buy from a reputable ticket seller

Organisers will include the details of the approved and official ticket seller for their event. So when purchasing, double check that it is the correct and authorised platform to avoid ticket fraud.

There are a select number of websites in South Africa that are most commonly used by large sporting events and concerts because they have the right security measures in place to handle these transactions safely. This includes payment portals that are secure, ensuring your information and credit card details are protected from cybercriminals.

2. Double check the website address

Fake websites can be easily recreated by scammers around an event to lure unsuspecting victims in handing over their hard-earned money and private information. Before entering any personal or financial details, make sure the website is secure.

A secure website will have a URL that starts with “https://” and a padlock to the left of the site address. This indicates that the website encrypts the data that you send and receive and makes it harder for hackers to intercept or steal this information. If these features are missing or your browser warns you that the website is not secure, do not continue with the transaction and leave the site.

3. Be wary of phishing emails and SMSes

Cybercriminals will often pose as legitimate organisations such as banks, delivery services or ticket sellers using fraudulent emails, SMSes or WhatsApps. These phishing scams will then try to encourage the user to click on a malicious link, which can either open an infected attachment, or send them to a website to hand over sensitive information like passwords, or credit card details.

Avoid falling victim to a phishing scam by checking who the message is from. If you don’t recognise the name or number of the sender, don’t click on any link in the message. Other key features of a phishing message include bad spelling and grammar, as well as a tone that tries to create a sense of urgency. It’s safer to not reply to the message with any personal information, and rather ignore and delete the message if it appears suspicious.

4. Use a strong password and activate 2FA

When signing up for a ticket seller’s website, you’ll often need to create a profile with a username and password. Use a strong password that can’t be easily guessed by a hacker. Try to ensure that the password is at least eight characters and includes letters, numbers and symbols.

Some websites might give you the option to activate two-factor authentication (2FA). This is a great way to add another layer of security to your account. Should a hacker acquire your login details, 2FA prevents them from gaining access by sending a one-time pin or code via SMS or email. Without this code, they cannot access your account.

2FA is also a great way to alert you to suspicious activity on your account. If you receive a one-time pin that you haven’t requested, you can alert the website and change your password to prevent them from signing in.

“It’s great to be back at live events, enjoying time with friends and family,” says Tzingakis. “And buying tickets online to our favourite matches and concerts is often the only way we can make sure we secure our seat to these festivities, but it can leave us exposed to cyber risks. It’s vital that we stay vigilant so as not to fall victim to online ticket fraud or phishing scam. With some basic digital hygiene habits and cybersecurity awareness, consumers can stop cybercriminals in their tracks.”