Five Tips to Avoid Online Shopping Scams

Zakir Hussain shares five simple tips to enjoy hassle-free shopping at a time when online scams are on the rise.

E-commerce is booming, and with it, a concerning number of consumers across the world are falling victim to cybercriminals and scammers. Purchasing gifts, tech ware or beauty products online is very convenient, but it can be risky if you're not paying attention.

From fake products and discounts to credit card fraud and identity theft, a frightening array of dangers can creep up on unsuspecting consumers. Today, we're brushing up on the best practices to spot and prevent online scams when shopping.

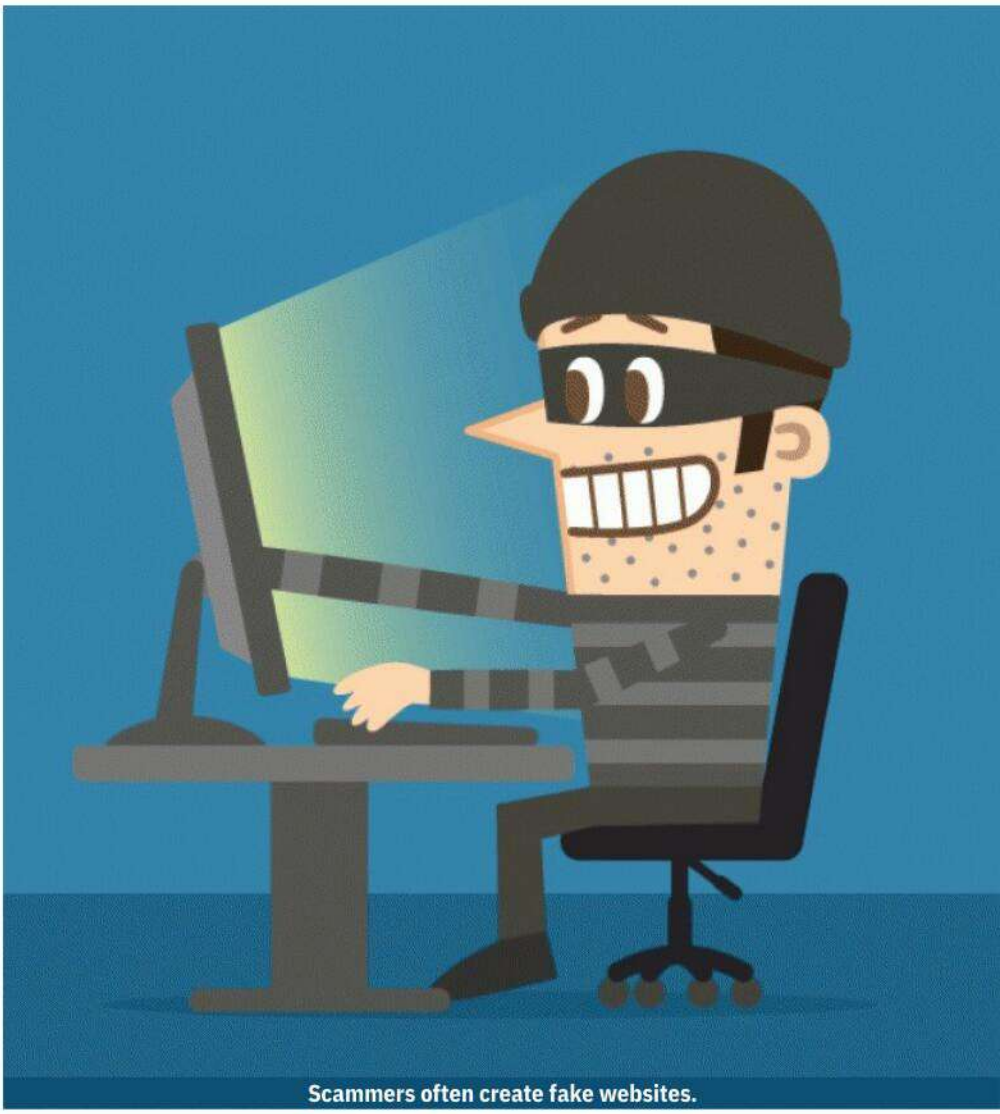
Do your research

When stumbling upon a new shopping platform online, it's important to do some research before handing over your credit card details. Scammers often create fake websites that mimic legitimate retailers to steal consumers' data.

Always check URLs of websites and webpages for typos or grammar mistakes. Never trust webpages that don't provide SSL encryption. Look for a green padlock icon at the start of the address bar or make sure the address starts with HTTPS instead of HTTP before buying anything from an online store. You can also check for customer reviews online, but don't believe everything you see in a comment section on social media platforms such as Facebook.

Be wary of information required at checkout

E-commerce platforms usually ask for particular information on checkout, including payment details, delivery address, phone number and email. Additional requests for information such as a PIN or Social Security number raise a big red flag. Of course, never send or give your credit card information to strangers or individuals promising you a great deal.



Scammers often create fake websites.

Be suspicious of gift card offers and coupons in your Inbox

Retailers often send customers special offers via email, including gift cards and coupon codes they can use on their next purchase. Scammers are also aware of this and send fake emails with phishing links to steal from unsuspecting users. If an email or offer you receive sounds too good to be true, treat it with suspicion. Search for the offer in your browser or contact the business directly. Some of these "special" deals also come with a request for users to complete a quick survey, a popular way for scammers to steal personal information, especially during the pre-holiday season.

Links and attachments in phishing emails can also deploy spyware and other malicious software that will allow a fraudster to harvest your sensitive data to compromise accounts and steal your money.

Always check URLs of websites and webpages for typos or grammar mistakes. Never trust webpages that don't provide SSL encryption. Look for a green padlock icon at the start of the address bar or make sure the address starts with HTTPS instead of HTTP before buying anything from an online store.

Consider changing your passwords before shopping

Digital hygiene is a must when shopping online. Make sure to set up an exclusive password for each platform, and enable any form of two-factor authentication. You can avoid account hijacking easily, and, in case of compromise, ensure that no other accounts are affected.

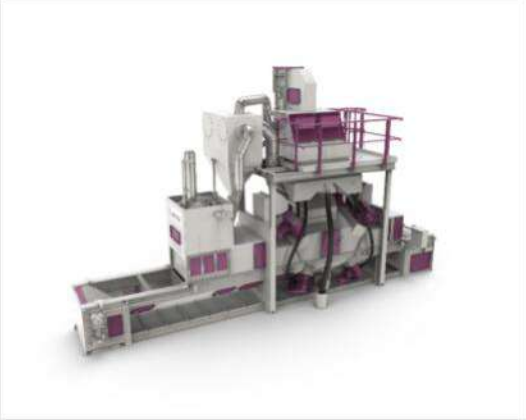
Secure your devices

Online accounts are not the only ones that need special attention when it comes to security. Keep your devices up to date and use a security solution on your PC, smartphone or tablet to protect against malware attacks, phishing attempts and fraudulent links.

Follow the simple steps, and enjoy shopping hassle-free!

Zakir Hussain Rangwala, Chief Executive Officer, BD Software Distribution Pvt Ltd has been engaged in IT, Channel Sales & Management since 1989. He is experienced in selling concept based products and services, products via digital downloads.

Optimum shot blast technology for castings



The surface treatment of complex cast workpieces made from aluminium or magnesium continues to become ever more sophisticated. The reproducibility of the shot blasting process for mass-produced parts is of particular importance in this context. Visitors will gain an overview of how reproducibility is taken into account during the conception phase and how it is put into practice.

AGTOS (A Gesellschaft für Technische Oberflächen Systeme) has designed and developed special shot blasting systems for treating lightweight parts and aluminium and magnesium castings. Aluminium is also often used as an abrasive material. Explore what we have learned in the process.

When investing in a shot blasting system, the overhead costs are of vital importance. The AGTOS Service APP addresses digital development and provides new customer benefits. It is available for download at the usual Android and Apple stores.

Using the app, AGTOS service technicians can give tips and instruction in the case of maintenance and repair work. These can be translated simultaneously on request. The service technician sees exactly the same as the person onsite. This way, the situation can be best appraised and analysed. Supplementary documents such as drawings, illustrations and photos can be shared to provide detailed explanations. The entire activity is documented so that it is available for later digital (replay) purposes. Test the possibilities directly at the exhibition stand.

The power of existing shot blasting machines can be increased so that turbines specially designed for this purpose work more gently. The abrasive consumption is reduced. The exhibition team will also provide more information.