

Online shopping is very safe... if you know what to look out for

Guy Raymond El Khoury, CEO of Accomplish shares his thoughts and suggestions for safe online shopping.

LONDON, LONDON, UNITED KINGDOM, November 17, 2022 /EINPresswire.com/ -- One element which existed prior to and grew exponentially during the pandemic was online shopping. What also grew alongside this was an increase in online fraud techniques. As we come up to the festive season, online fraudsters will ramp up their efforts as people shop for family and friends.

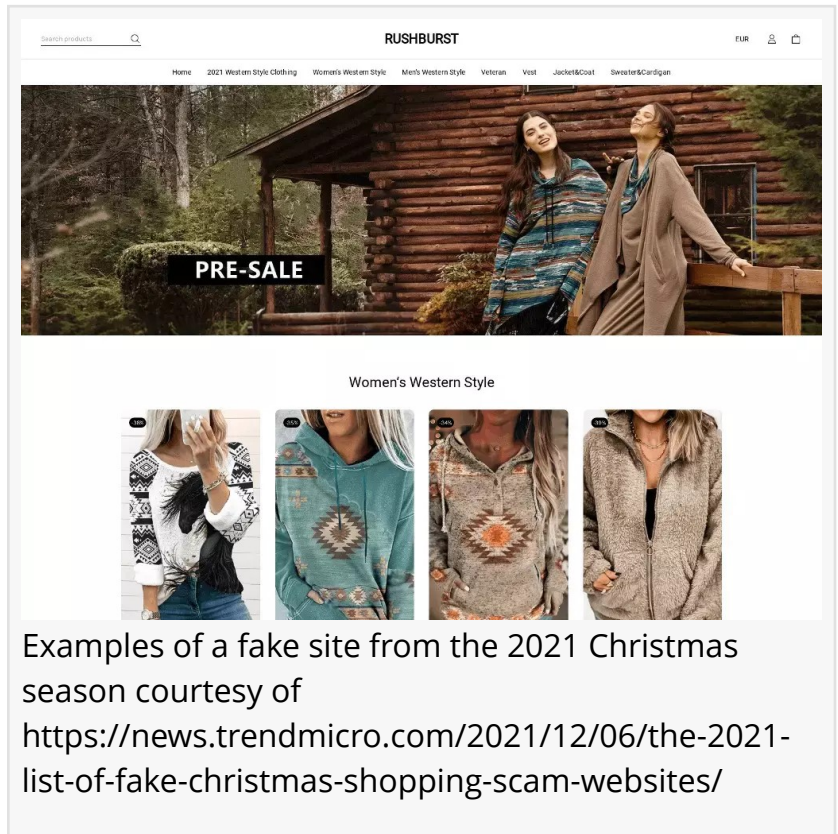
As [Accomplish](#) (formerly Accomplish Financial) is a leading payments technology company, it believes it is crucial to share its knowledge and expertise to ensure consumers and reputable online retailers enjoy safe and secure online transactions. According to CEO, Guy Raymond El Khoury, there are some golden rules to follow and a few red flags to watch out for:

“

Know the rules, spend a little extra time checking out websites before buying and make sure your security isn't compromised or that your purchase will arrive.”

Guy Raymond El Khoury

the site has a valid certification.



-“Always make sure the website you're looking at is legitimate.

-Does the website accept payment cards or a trusted payment method that allows you to dispute a transaction in case of a problem? (Hint: good card issuers should allow you to do this!)

-Make sure the website uses SSL (usually designated with a padlock icon in the address bar).

-Click on the padlock at the drop-down menu to check if

-Look out for small differences in the site's URL (web address). It might just have an added letter or a slight spelling change. For example, Guccii instead of Gucci.

-Have a good look at the e-commerce site to see whether it's professionally produced or 'thrown together'. Again, whether there are typos, grammatical mistakes and poor-quality images

should give you a clue to its authenticity. Another essential check is whether they are easily contactable and want to tell their 'about us' story.

-You can always look on a search engine for reviews of the company – what you find might instantly confirm that it's genuine or prove it's a scam.

-Always work with reputable merchants.

-Look for a certificate of authentication with a 'trust mark' on the footer, header or checkout pages of the website that actually links to a certificate (i.e. is not just a picture).

-Some copycat websites do deliver your goods – but these are inferior quality knock-offs not even worth the discounted rate you've paid. Many European countries consider the purchase of such goods illegal and impose heavy fines on the recipients.

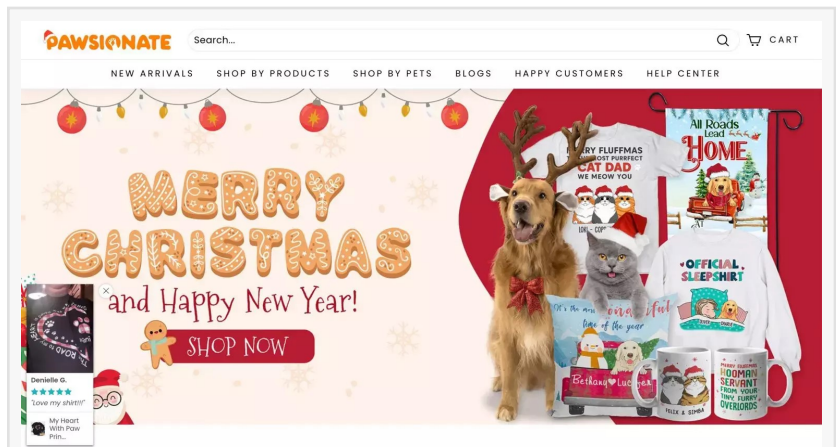
-Fake reviews – do the reviews look suspiciously similar or badly worded, yet all giving the highest rating?

-Unusual payment methods (wire transfer/cash etc.)

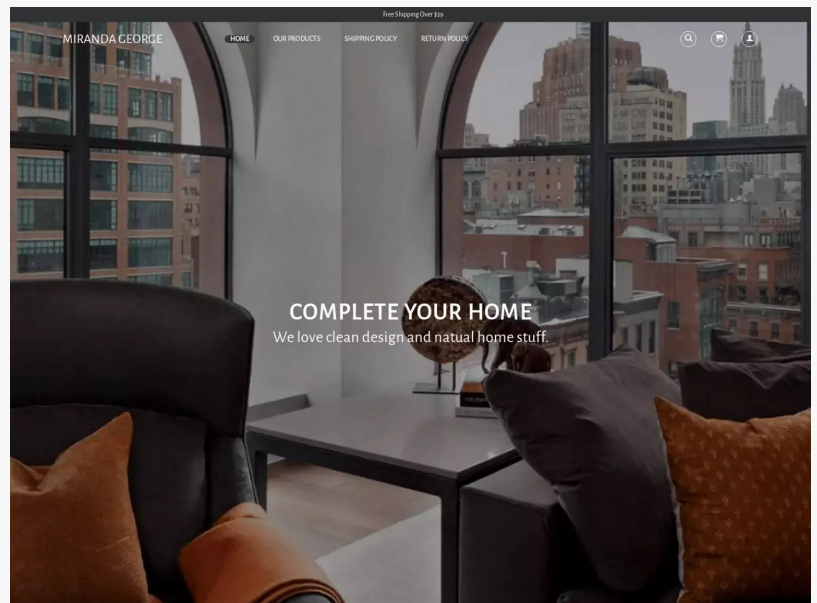
-Too much detailed personal info is required that has nothing to do with what you are buying or its delivery."

"The bottom line," adds El Khoury, "is that if the offering is too good to be true then it inevitably is. There's no such thing as merchants practically giving things away or special offers at a fraction of the price everywhere else."

Other elements to consider:



<https://news.trendmicro.com/2021/12/06/the-2021-list-of-fake-christmas-shopping-scam-websites/>



<https://news.trendmicro.com/2021/12/06/the-2021-list-of-fake-christmas-shopping-scam-websites/>

LAYERS OF SECURITY

“As an issuer, we are always trying to implement the latest technology to protect account holders. We were one of the first companies to implement 3D Secure Version 2 which card schemes such as Mastercard and Visa adhere to and recommend. This adds an extra layer of protection to online shopping as with 3DS enabled cards you have a two-step authentication process for every online purchase. No payments will go through unless you authorise them yourself.”

“Most people by now have experienced some form of SCA (Secure Customer Authentication) where you receive an SMS or email with a one-time code to enter in order to complete your purchase.”

The new evolution is biometric authentication, where you can confirm your identity by you looking at your phone (face recognition) or using your fingerprint. These evolutions in technology increasingly make it difficult for fraudsters, particularly if your payment card is stolen. “It is important to note that whilst in the UK advanced standards are implemented, there are some websites in different parts of the world that may not adhere to these standards, so once again check security and make sure you are making purchases with legitimate merchants” adds Guy El Khoury.

VIRTUAL CARDS AND TOKENISED CARDS

What makes card and purchasing security even stronger are virtual cards with no plastic involved. “A virtual card is essentially card details without the plastic card. Virtual cards can be issued quickly, used and the credentials discarded, even just for a single purchase,” explains Guy Raymond El Khoury. That means that although this ‘card’ works in the same way as normal for online transactions, if you wish the card number can never be issued again. You can also use virtual cards to manage expenses, budgets or even spending at specific merchants by assigning each one a different virtual card .

“To take security to a whole new level, using many of the existing concepts, where we want to end up next is tokenisation. Your transaction is linked to a token rather than a card number. The token is randomly generated at the moment of use and identifies you, the network, and financial institution to the merchant for a single purchase, and then once the purchase is done, the token immediately becomes redundant. This doesn't even have to be in a traditional 16-digit card form, it is more like an encoded layer to the transaction without you having to give your card details or credentials.”

This concept can be found in the digital payment technology used by Apple Pay and Google Pay, for example.

CONSUMER PROTECTION

According to Guy Raymond El Khoury, The UK and European consumer's rights are currently

well-protected. "Financial institutions have enforced regulatory requirements in place, looking out for your rights. If your phone is stolen or compromised there's an extremely good chance that you're covered. Even if you already have that cover this is an additional safety net. If fraud is suspected through a transaction, you know nothing about, then they may still investigate, but with the consumer's protection in mind."

So, know the rules, spend a little extra time checking out websites before buying and make sure your security isn't compromised or that your purchase will arrive.

Guy Raymond El Khoury

Accomplish

[email us here](#)

Visit us on social media:

[LinkedIn](#)

[Other](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/601851650>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2022 Newsmatics Inc. All Right Reserved.