

Brushing scammers have a different notion of give and take: Cyber-Forensics.net beware of scammers sending mystery gifts

Brushing scam involves sending mystery gifts to people they didn't order. It's a technique to exploit search engine rankings and steal information.

SOFIA, BULGARIA, March 16, 2022 /EINPresswire.com/

-- Brushing scammers have a different definition of give and take: Cyber-Forensics.net beware of scammers sending mystery gifts

Brushing scam involves using third-party vendors like Amazon to send products people didn't order. It's a technique to exploit search engine rankings and steal information.

Brushing is an old technique used by sellers where they pay money to fake buyers to write reviews or buy products and improve their positions on eCommerce websites. However, modern-day scammers have begun taking advantage of this old technique to steal consumer information, use it in identity thefts, and even sell the data on dark webs.

Reportedly, a total of one million people have already been targeted by a series of brushing scams. And the uptick in the cases has caused prestigious organizations to issue urgent warnings.

Cyber-Forensics.net, a [fund recovery](#) service company meant to aid online scam victims, estimates that around one million more households are under threat of brushing scams.

Chief analyst Timothy Benson says: "brushing scams have raised concerns worldwide. Some scammers create fake accounts to encourage genuine buyers to provide personal information online." This data can be exploited at many levels.

How Do Brushing Scams Work?

Fund recovery expert Peter Thompson explains how brushing scams are pulled off? A person receives a package from an unknown source containing items that the consumers never requested. The package includes the recipients' names but no return address.



Cyber-Forensics.net



Cyber Forensic Specialist

“

brushing scams have raised concerns worldwide. Some scammers create fake accounts to encourage genuine buyers to provide personal information online.”

Timothy Benson

The sender of the item is usually an international company or a third-party seller. Successful delivery of the items tends to convert the package recipients into verified buyers on marketplaces.

The scammers then use the verified buyers' personal information to post false product reviews online. This ultimately boosts 5-star ratings of the company online to encourage potential shoppers to order the article after discovering positive reviews. More customers mean more

consumer data to exploit.

And since the merchant companies receive a cheaper product, scammers perceive this as an excellent opportunity to steal personal information.

Meghan Atkinson's experience with the brushing scam started last summer. Atkinson received a package from Amazon to her home. The box contained a dog pool which seemed out of place considering Atkinson didn't own any pet.

She scoured her order history, thinking she may have ordered it accidentally. But when she looked at the online cart, there was no trace of the product. However, when the packages kept coming, Atkinson feared the worst: an online scam on its way.

She told the local authorities, "We got a smartwatch. I've had phone cards for Apple products, but I don't have Apple Products. I received vacuum bags. And they're just sitting around."

According to account recovery specialist Peter Thompson: "anyone receiving unsolicited packages from overseas or shipped from random places could be at a potential risk of losing privacy."

Experts also advocate that consumers should take these as warning signals that personal information might be in the hands of potential hackers.

Chief analyst Timothy Benson says, "Brushing scammers might get the consumer information and link it to illegal websites. Details like names, address, phone numbers could also be ordered around the dark web and sold online."

These days nobody is immune to brushing scams. So as a consumer, it is the duty to protect information and make sure the users implement the best protective measures to stay safe.

How to Avoid Being Victims of Brushing Scams?

Never pay for unrequested orders: Peter Thompson says, as per law, recipients need not pay for

packages they never ordered, even when the package delivering company forces the recipients.

The receivers are under no obligation to pay for such merchandise, and they can consider it a gift. If the receipts don't want the item, they can donate it or dispose of it.

Report any unrequested packages arriving at the door: If the recipients get anything delivered at their door when they didn't, order-especially if it is something like an organic item like seed, plant, or food. It's advised to report the matter immediately.

Organic items like seeds can be noxious weeds or carry diseases that could damage essential plants or crops. Also, the recipients should ensure the package is sealed correctly to make sure there was no tampering on its way.

Notify the retailers: If the package received belongs to a third-party retailer like Target, Walmart, Amazon, it is advised to report the matter to the retailer to remove the reviews under the recipient's name if any.

Monitor account activity regularly: When someone receives such unordered packages, the customer's personal information may have already been compromised through illegal means.

Scammers can run illicit activities using this information. Therefore, it is recommended to carefully examine all the online shopping accounts and check the credit card bills. Check for unusual signs of fraud activities or forex withdrawal problems.

Change Password: If the victims' account has unidentified order confirmation, immediately change the passwords on the shopping apps.

How To Ensure Information is Safe From Getting Stolen?

[Fund recovery companies](#) recommend that the best way to secure user information from being misused by scammers is to practice the best internet surfing approach. For example:

Never click unknown links.

Check the sent URL links through SMS, emails, Texts.

Using a two-step authentication strategy.

Using only secure servers to browse the internet.

Use only legal platforms to make payment.

Securely close all tabs, and sign out of all accounts,

About Cyber-Forensics.net

Cyber-Forensics.net is committed to providing the most accurate tracing service for victims of online scams. Cyber-Forensics.net empowers and simplifies the process of tracking down the cyber-criminals and assists in recovering the funds and creating an atmosphere for a negotiated settlement. For more information, please visit <https://cyber-forensics.net/>.

Peter Thompson
Cyber-Forensics.net
+1 917-920-6613

[email us here](#)

Visit us on social media:

[Twitter](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/565051863>

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 IPD Group, Inc. All Right Reserved.