www.simplemailprotection.com

FRAUD PREVENTION GUIDE

HOLIDAY EDITION 2020

Trustifi

CONTENTS

INTRODUCTION

The holiday season is also the phishing and scams season as attackers leverage the increased use of online shopping to get credentials or money. This increase will likely be more dramatic this year due to the COVID-19 pandemic. With an increase in people staying safe at home, more shopping will be done online rather than in physical stores.

PURPOSE

This guide will provide warnings against common scams and recommendations for safe behavior on the web during the holidays.

Trustifi

SCAMS TO BE AWARE OF

Trustifi's data shows that there is an increase in phishing, spam, and Business Email Compromise (BEC) attacks. These scams might not be easy to spot since the attackers always figure out new creative ways to trick users. Unfortunately, these scams could lead to credential harvesting or the theft of credit card numbers and even money.

HOW THESE SCAMS WORK

Phishing Attack is when the attacker is masquerading as a trusted entity (person, store, or service provider), making the victim trust them, and hand over sensitive information.

Spam is usually an unwanted email, usually advertisements. Spam emails can contain phishing – the attacker sends an advertising email and adds a link to a phishing website to lure you in.

Business Email Compromise (BEC) is a scam used to impersonate an important, valuable, known person to trick the user to take certain actions. Usually, BEC targets companies and impersonates the CEO. The email is sent to an employer and asks for an urgent wire transfer, invoice payment, or gift card purchase.

TOP HOLIDAY SEASON'S ATTACKS

1. **Fake deals** – spam, advertising emails, offers on "too good to be true" deals. Often also mimics popular stores.
2. **Fake receipts and invoices** – using phishing techniques, the attacker sends a fake receipt or invoice to catch the recipient's interest ("interesting... I don't remember I bought this product") and make them click a link or download the malicious attachment.
3. **Fake shipping status alerts** –Shipping status emails can incite the recipient's excitement to get their shipment and make them click a forged link to track the shipment. But instead of tracking shipment, their computer might be infected with malware or they can be asked to fill in their personal details.

> Every step of the online shopping process can be compromised with sophisticated social engineering and spoofing techniques.

Mark L.
Information Security, Compliance and Data Protection Officer, **Trustifi**

Contact Us:
www.simplemailprotection.com
855-958-0754
Sales@SimpleMailProtection.com

Trustifi