Watch out for **Phishing Emails and Cyber Security Risks during the Holiday Seasons**

Welcome to our Cyber Security Newsletter! In this issue, we want to discuss being extra vigilant when checking your email during the holiday season. With online shopping at an all-time high in 2023 and more frequent use of **digital payment methods** than ever before, cybercriminals are actively looking for victims to target through malicious phishing emails.

Research from **Cyber Security Ventures** has found that businesses worldwide have seen a **350%** increase in **phishing scams** since last year, meaning now is an especially critical time to ensure your security protocols are up-to-date. Furthermore, studies conducted by **Comodo** show that one in every **143 emails** sent this year globally will be identified as malicious – highlighting just how prevalent these threats are today.

You must know the key things to watch out for if you want to protect yourself against these risks and **stay safe online** during this busy festive period.

Understanding Phishing Emails

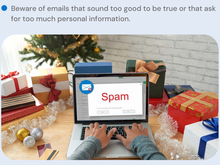
Phishing is the fraudulent practice of sending emails that appear to be from reputable sources such as financial institutions, government agencies, and online merchants.

The aim of phishing emails is to trick people into clicking on links or attachments that install malware on their computers or direct them to a fake website where they are asked to submit personal information.

How to Spot Phishing Emails

Phishing emails can be difficult to detect, but there are some telltale signs that can help you identify them.

- First and foremost, you should scrutinize the email's sender address and domain name carefully. Look out for misspellings, odd characters, and unrecognized domain extensions.
- Check the email's content for grammatical and spelling errors, and generic greetings like "Dear customer" instead of your name. Always hover your mouse over links in the email to see if the URL matches the text.
- Beware of emails that sound too good to be true or that ask for too much personal information.



Unwrapping the Threat: A Deep Dive into Common Holiday Phishing Attacks

1. Fake Order Receipts: Cybercriminals send fraudulent emails that appear to be purchase confirmations from popular e-commerce sites. The emails often contain a link leading to a malicious website that steals personal information.

2. Spoofed Tracking Shipments: Scammers send deceptive emails posing as shipping companies, claiming there's an issue with the delivery of a package. The emails usually contain a link that, when clicked, can lead to the installation of malware or the theft of personal information.

3. Falsified Charitable Contributions: Cybercriminals take advantage of the season of giving by sending emails that impersonate legitimate charities. These emails often ask for donations and provide a link to a fake website where they collect personal and financial information.

4. Social Media Scams: According to Norton's research, cybercriminals primarily targeted victims during the holiday season through social media platforms. They lure victims into clicking malicious links or sharing sensitive information under the guise of holiday promotions or contests.

5. Retail Phishing and Ransomware Attacks: With the onset of the holiday shopping season, hackers have increased their phishing and ransomware campaigns targeting the retail sector, aiming to steal financial data and disrupt services.

6. The "12 Scams of Christmas": This involves a range of scams that are common during the holiday season, including gift card scams, e-card scams, and fake shopping websites.

The Impact of Phishing

With increased online shopping, cybercriminals are out in full force, looking to steal personal information and wreak havoc on your finances. The impact of phishing during the holiday season can be disastrous, causing stress and financial strain on families already dealing with the challenges.

What to Do If You Receive a Phishing Email

If you receive a phishing email, the best course of action is to delete it immediately. Do not click on any links or attachments, and never provide personal information or financial details.
If you are unsure whether an email is legitimate, contact the sender using a verified email or phone number. You can also report phishing emails to the Federal Trade Commission (FTC), your bank, or your credit card company.

How to Protect Yourself from Phishing Emails

The best way to protect yourself from phishing emails is to be proactive and diligent. Regularly update your computer's security software and keep your operating system and web browser current.
Use strong passwords and enable two-factor authentication where possible. Never use public Wi-Fi networks to access sensitive information, and be wary of emails that ask for personal or financial information.
Lastly, educate yourself and your family and friends about the risks of phishing emails and how they can stay safe online.

Extra Measures for Cyber Security

It's no longer enough to have a strong password simply; we recommend implementing two-factor authentication for an added layer of security. Additionally, ensuring that your network is secure is critical for safeguarding sensitive data.

But it doesn't stop there – keeping your software up to date is equally crucial. Regular updates ensure the latest patches are in place and often contain enhanced security measures. In today's digital world, taking every step possible to secure your online presence is essential. Stay vigilant, stay safe.

Summing it Up

As we wrap up this edition of our newsletter, the key takeaway is the importance of vigilance in protecting ourselves from phishing emails and various cyber threats, especially during the holiday season. With cybercriminals becoming increasingly sophisticated, it's crucial that we stay one step ahead by being informed and exercising caution in our online interactions.

Remember, always scrutinize emails for signs of phishing, such as poor grammar, requests for personal information, and unfamiliar email addresses. Be wary of clicking links from unverified sources, and ensure your antivirus software is current.

Embrace the joy and generosity of the holiday season, but let's also prioritize cybersecurity. After all, the greatest gift we can give ourselves this festive period is peace of mind, knowing that our digital lives are secure.

Stay safe, stay vigilant, and happy holidays from all of us here at Microsys.