HOLIDAY 2019

AVOIDING CYBERTHREATS THIS HOLIDAY SEASON

Salvus TG

INTRODUCTION

This holiday season, more than ever, it is crucial to know how to protect yourself from cybercriminals. With the consistent increase of online holiday shopping, these bad actors are ramping up campaigns to steal your money, data and personally identifiable information. In this short handbook, we will provide insight to keep you safe while shopping and browsing online and show businesses how to keep their customer data protected.

Table of Contents:

CONSUMER STATISTICS

56%

Of holiday shoppers plan to make purchases online in 2019

43%

Of online shoppers surveyed said their identity theft was due to holiday shopping online

8%

Of consumers surveyed in 2018 stated that they were victims of identity theft during the holiday season.

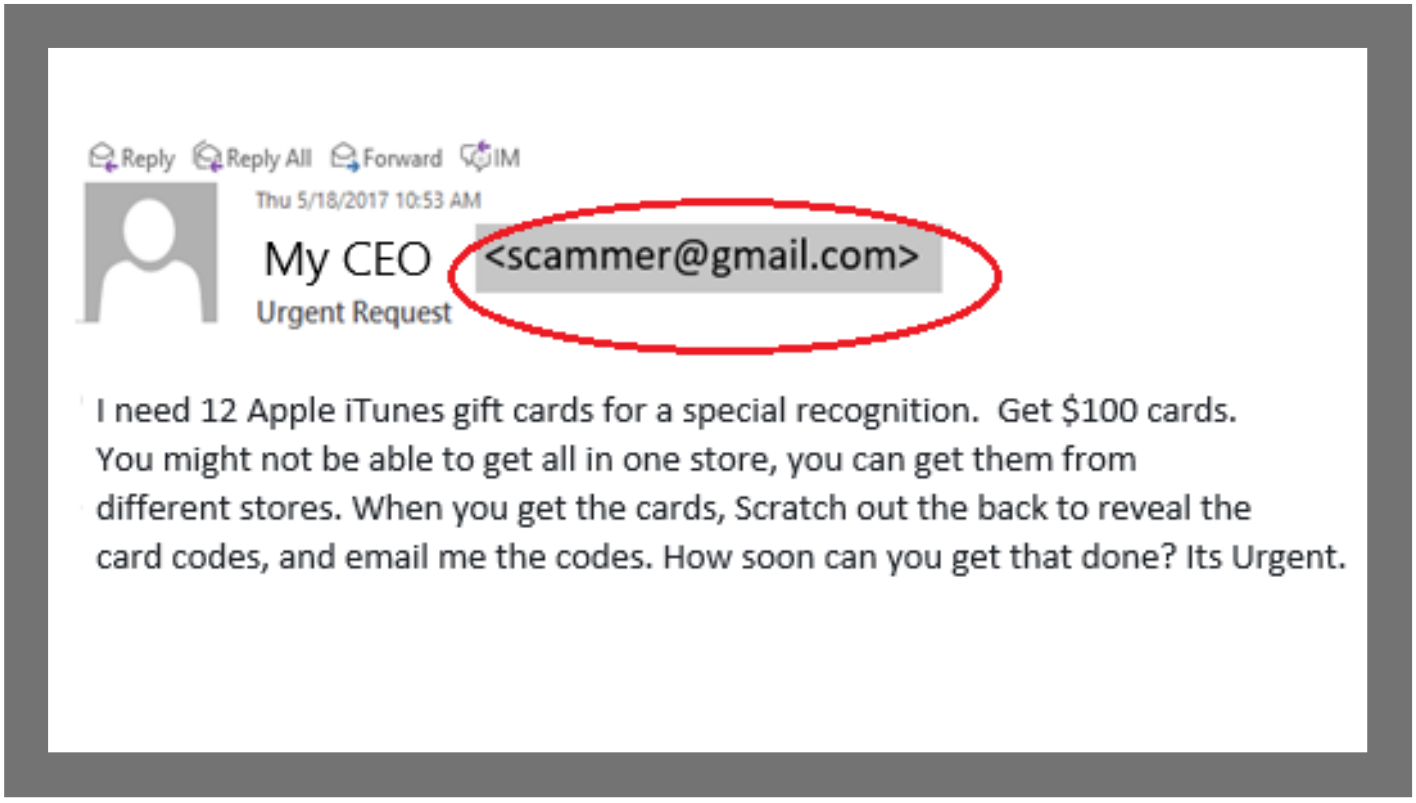
Statistics sourced from Norton by Symantic

BUSINESS ADVICE

Impersonation Attacks

At the end of the year many contracts are expiring and invoices are being paid. The increase of financial transactions gives cyberattacks an opportunity to go unnoticed until it is too late. A favorite of cybercriminals is the **Impersonation attack**.

Impersonation attacks, also known as CEO fraud, starts by targeting an executive in an organization. Fraudsters attempt to isolate an executive and steal their login credentials. With these credentials they are able to perform a CEO scam. CEO scams occur when an email, seemingly addressed from a CEO or other member of senior management, is falsely created by a scammer in order to exploit the trust of employees. The impostor email seeks for the target to wire funds, purchase gift cards or share confidential information with the scammer.



BUSINESS ADVICE

Working Remotely

Now is the time to ensure that your employees understand current cybersecurtiy policies. With increased traffic and increased cybercrime, it is critical that staff is familiar with all established security procedures.

This includes how to protect company information when accessing it from a remote site. Remind staff to avoid insecure and public Wi-Fi networks and to use a VPN whenever available to secure their outside connection to your business network.

Personal use of Business Systems

The popularity of online shopping around the holidays increases the number of fraudulent websites that are created to scam customers. These sites can house malware and viruses that can infect your business network.

If employees are allowed to use business internet for personal use, make sure they are aware of these dangers and know how to validate a website is legitimate. You should double check the spelling of the website, (e.g. **amazon.com** vs **amaz0n.com** that has a zero instead of an O) and look for the lock icon in the URL bar to confirm a secure connection.

CONSUMER PROTECTION

Holiday Scams

The holiday season is rich with its own unique scams to look out for. Here are some common characteristics of these scams:

Poor grammar or spelling - Read all emails closely and look for any grammatical mistakes. Scam emails are typically filled with errors. If you notice multiple instances of poor grammar, it is most likely a scam.

Unfamiliar Sending Address - Scam emails will often come from an odd email address. Typically with a string of letters and/or numbers that don't quite make sense. These emails will also use odd terms or titles in the body of the email like MAIL CONTROL UNIT or AMAZON CHRISTMAS TEAM.

Donation & Charities - Scammers will take advantage of holiday cheer and pose as a legitimate charity looking for contributions. Instead of replying to the email, navigate to the charity's website via Google or by typing it into the URL bar manually if you wish to donate.

Deals & Coupons - Cybercriminals will take advantage of those looking for a good holiday deal. Scrutinize any deal or coupon that seems too good to be true. It usually is. You can always reach out to the brand's customer service team and ask them to confirm if the coupon is legitimate.

CONSUMER PROTECTION

Password Best Practices

Passwords are one of the most commonly implemented security solutions. They are a basic, often mandatory, bare minimum approach to security. But when they are strong, a good password is one of the easiest ways to defend your data. A recent Verizon Data Breach Report states that **"81% of hacking-related breaches leveraged either stolen and/or weak passwords."** The following tips should help reduce your risk of breach.

Avoid the Obvious – Password1! or LogMeIn have been used and used again. Cybercriminals have a database of commonly used passwords, if yours is on the list, you are not secure.

Use Different Passwords for Different Accounts –You should always use a different password for different accounts. Your email password needs to be completely different than your Amazon account. So Hunter2 and Hunter3 is not different enough to be considered secure. This way, if one password is leaked or stolen, not all of your accounts are compromised.

Change Passwords Often – This one is easy, change your password every 90 days. If your password is leaked or stolen, simply changing it regularly can mitigate the risk of a breach.

Use a Password Manager – If you want to avoid having to constantly change and remember different passwords for different sites, you can utilize a password manager. These tools will create very strong passwords for all of you accounts. As long as you create a strong password for the "master password" you will only have to remember one password ever again. Check out Dashlane or LastPass if you are interested in a free password manager.

Turn on Multi-Factor Authentication - Multi-factor authentication adds an extra layer of security to your online accounts. In addition to a password, you will typically need to input a one time code you receive from a text message. This will keep attackers out of you accounts even if they have your password.

CONSUMER PROTECTION

Safe Shopping & Shipping

When shopping online, make sure that you are on a legitimate e-commerce site. If you are unfamiliar with the site, do a bit of research. Checking for reviews is a great way to make sure the site is safe. If a site has no reviews that is a good indication of a it being fraudulent.

Use credit cards to make purchases. Better yet, use just one card if you can. Credit cards have more built in protection than debit cards. So in case of issue, you can mitigate loss.

Be wary of any shipping or package tracking emails. With so many different online purchases being made it is easy to lose track of what is on order. Scammers will send emails that look like shipping updates in hopes you follow a bad link or provide personal information.

Ship all packages to a secure location. The holiday season brings out the "porch pirates" that are looking to steal you deliveries from your front door. Consider shipping your purchases to your office or utilize secure lockers that are now available from Amazon, UPS and FedEX.

Secure Connections

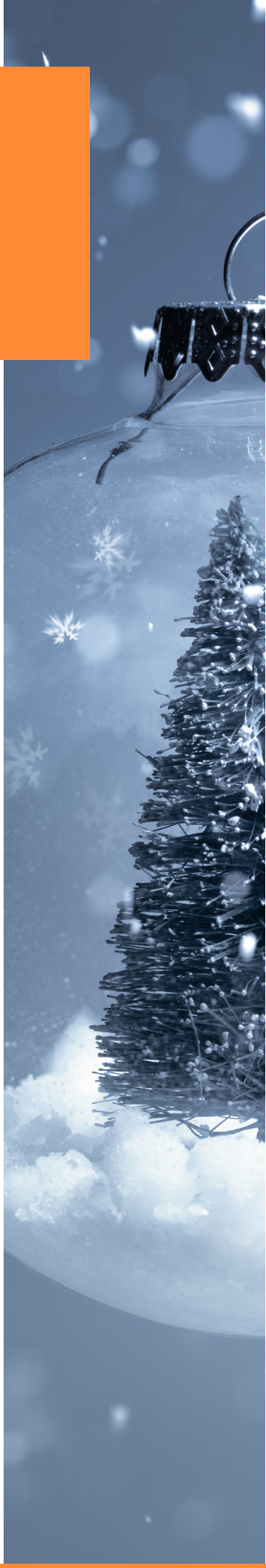
Avoid Public Wi-Fi -

While it may be convenient to do some holiday shopping from a coffee shop or make a last minute purchase from the airport, public Wi-Fi networks can be dangerous. The biggest risk when using public WiFi is known as a **Man-in-the-Middle attack.** Equitable to eavesdropping, cybercriminals sit in-between the access point and the end user, spying on or copying data that is passed back and forth. So, if you sign in to your email or make a purchase, the “man in the middle” can see it too.

Use a VPN -

If you do decide to shop online using public Wi-Fi, consider using a VPN on all your devices before connecting to any public Wi-Fi network. A VPN creates an encrypted connection between your devices and a VPN server. Think of it as a secure tunnel that internet traffic travels through while you shop, making your data more difficult to intercept.

CONSUMER PROTECTION



Social Media

A common assumption is that your privacy settings are properly configured for all social media profiles. What you may not know is that social media app updates or changes could revert your profile to public. A public profile gives cybercriminals an opportunity to mine data from your profiles and use that data to compromise other accounts. It is good practice to review your social media privacy settings often.

Criminals are also watching your profiles in hopes that you will post travel plans for the holiday season. Broadcasting the fact that you will be out of town lets criminals know that no one will be home. This can encourage a would be burglar to attempt a break-in. This also presents an opportunity for a cybercriminal to scam your family members or conduct fraud. Knowing that while you are on vacation you will be less likely to keep tabs on your financial accounts.

Review Financial Statements

It is crucial to monitor bank and credit cards statements regularly during the holiday season. Scams are becoming more and more sophisticated and the impacts can easily go unnoticed.

Some financial institutions and credit card companies provide account monitoring and alerting. Research your bank and credit card companies and turn on alerts if they are available. This way you can quickly combat fraudulent charges.

CLOSING THOUGTS

CYBERSECURITY IS A YEAR ROUND COMMITMENT

While there are times of the year that cybersecurity awareness should be heightened, it is a risk year round.

Businesses and individuals should continue their vigilance against cybercrime everyday. The old adage, ***it is not if, but when***, rings true when it discussing cyberattacks.

To effectively combat the bad actors that look to steal your data and dollars, it is crucial to stay up to date and informed on the latest security trends.

Just remember, keeping systems up to date, employees and family educated and security top-of-mind is the best defense against these threats.

For further security advice, informative guides and articles, visit our website at www.salvustg.com/blog

Happy Holidays for all of us here at Salvus TG.