



Commonwealth Fusion Center (CFC) Massachusetts

(978) 451-3700 | (508) 820-2233



(U//FOUO) CFC Massachusetts Cybersecurity Program (MCP) Bulletin: 2020 Holiday Crimes and Scams 12/16/2020

(U) OVERVIEW

Source: Next Caller

(U) The holiday season brings an increase in online shopping and financial transactions, which leads to increased opportunity for criminals to exploit victims. During this time, cybercriminals alter their phishing attacks and other cybercrimes with holiday season themes. Phishing is a cybercrime in which an unsuspecting victim willingly gives sensitive information (personal, financial, business) to someone they believe is an official/legitimate institution or someone with whom they have a pre-existing relationship. The CFC Massachusetts Cybersecurity Program (MCP) has developed this bulletin for situational awareness purposes.

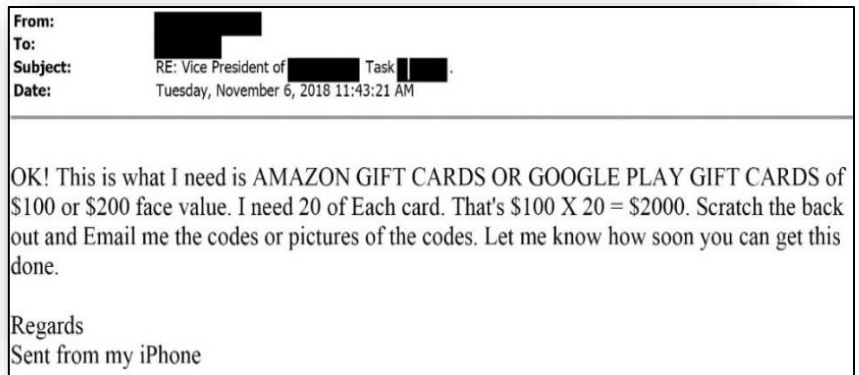


(U) HOLIDAY CRIMES AND SCAMS

Business Email Compromise (BEC) Gift Card Fraud

– BEC is when cyber criminals gain access to or impersonate email accounts that belong to high ranking or influential employees of organizations. BEC gift card fraud is when attackers impersonate an email account that belongs to a high-ranking official of a company and email members of the organization to encourage them to purchase gift cards to give as gifts to other coworkers for the holidays. By purchasing these fake gift cards, employees unwittingly give money and financial information directly to the cyber criminals.

Source: Roebuck Technologies



Red Flags



- * **E-mails from high-ranking officials (if out of the norm)**
- * **Links to unknown gift card websites**
- * **Generic emails that are not specific to your company or to you**

Unclassified//For Official Use Only

The information contained in this bulletin is For Official Use Only and is the property of the Commonwealth Fusion Center (CFC). It is intended for official use by law enforcement, public safety partners, and authorized critical infrastructure partners. No portion of this bulletin should be copied, released or re-disseminated without prior approval of the Commonwealth Fusion Center. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access. Information bearing the FOUO caveat may not be used in legal proceedings without first receiving authorization from the originating agency. Recipients are prohibited from posting FOUO information on a website or an unclassified network. Persons or organizations violating this policy will be prohibited from receiving CFC products.

Fake Charities and Donations – During the holidays there are numerous charitable causes and organizations seeking donations. Cyber criminals create their own fraudulent charity and donation websites designed to appear legitimate and similar to reputable organizations. Links to these malicious sites can also be sent to victims through phishing emails and texts.

Red Flags



- * **Broken English or multiple grammatical errors**
- * **Unusual domain name and web address**

Holiday Vacation Getaway - Many people may travel during the holiday season. This provides plenty of opportunities for cyber criminals to target people with fraudulent vacations or rentals. Most of these scams take place via the internet or text message with no face-to-face contact. Lures can include a variety of exciting deals on hotels and other rental properties. Scammers might offer a discount if the victim wires the money instead of booking online using a credit card, leaving the victim no way to recover their funds. Cyber criminals trick victims into believing they have booked a legitimate vacation or booked a rental property when the location does not exist or even belong to the person with whom they are dealing. Additional scams can include fake airline tickets, car rentals, and travel insurance.



Actual Disney themed scam. Source: Inside the Magic

Red Flags



- * **Winning a free vacation contest that you did not enter**
- * **False sense of urgency (e.g., deal ends soon, buy now!)**
- * **Vague responses about property when asked details about location**
- * **A deal that seems too good to be true**

Source: CBS News

Seasonal Employment – Package delivery services and retailers regularly hire additional seasonal workers to deal with the holiday demand. These jobs are a great way for people to make additional money during the holiday season. The increase in hiring advertisements can create more opportunities for criminals to scam people with fraudulent job offers. Cyber criminals could advertise fake job opportunities to lure unsuspecting victims. After the victims are selected and offered the job, they are then asked to provide banking information and personally identifiable information (PII) to begin the hiring process. Scammers may even state that new employees must pay up front for supplies and training expenses.

Red Flags



- * **Employers that ask for payment up front**
- * **Jobs that do not require an interview**

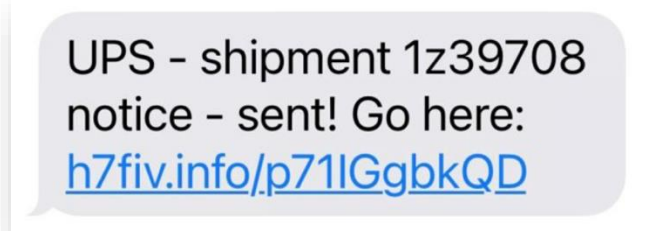


Unclassified//For Official Use Only

The information contained in this bulletin is For Official Use Only and is the property of the Commonwealth Fusion Center (CFC). It is intended for official use by law enforcement, public safety partners, and authorized critical infrastructure partners. No portion of this bulletin should be copied, released or re-disseminated without prior approval of the Commonwealth Fusion Center. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access. Information bearing the FOUO caveat may not be used in legal proceedings without first receiving authorization from the originating agency. Recipients are prohibited from posting FOUO information on a website or an unclassified network. Persons or organizations violating this policy will be prohibited from receiving CFC products.

Package Tracking - The increase in online shopping in 2020 and the subsequent increase in package shipments and deliveries provides additional opportunities for scammers to take advantage of people. Package tracking scams are normally done via email or text messages and can include a variety of malicious activity. In most cases, the message reflects a shipment confirmation and provides a link to track the delivery. These malicious links can direct victims to fraudulent sites or download malicious files to the victim's cellphone or computer. A new spin on traditional package tracking scams involves messages that confirm packages have shipped with a link to a customer satisfaction survey with the lure of a free gift if completed. At the end of the survey, victims are asked to provide credit card information to cover the shipping cost of the gift. In reality, victims have provided their credit card information to cyber criminals.

Source: Fox35 Orlando



Red Flags



- * **Message received without having placed an online order**
- * **Text received without providing cell phone number**
- * **Different shipping provider (i.e., confirmation e-mail states USPS but text says UPS)**

Typo Squatting & Fraudulent Sites – Typo squatting targets internet users who incorrectly type a website address in their browser. This typographical error may lead people to a malicious website designed to look like the legitimate site. Other variations of this scam involve malicious actors sending emails disguised as recognized vendors with links that lead to malicious sites.

Red Flags



- * **Broken English or multiple grammatical errors**
- * **Unsecured web address**
- * **Incorrect spelling or symbols used in web address**

Source: Twitter

Real Domain Targeted	Typosquat Domain Example
www.github.com	www.gIthub.com
www.google.com	www.gougle.com
www.amazon.com	www.amozon.com
www.homedepot.com	www.homdepot.com

(U) Social Media Cyber Hygiene

Posting Details of Future Vacations – People often post to social media about upcoming or current vacations. Criminals could use vacation details to plan a robbery knowing that the victims will not be at their home during this time period.


Posting Pictures of Extravagant Holiday Gifts – People tend to post pictures of gifts they have received or given to their friends and family. These pictures could motivate criminals into robbing the poster. This is the digital equivalent of putting packaging outside for recycling when it is clearly labeled with what was inside (e.g., boxes for flat screen TVs, video game consoles, or other expensive items).

(U) Recommendations and Tips

- Be wary of emails requesting personal information – Phishing emails try to trick victims into releasing important and valuable information (e.g., credit card information, PII, etc.). Attackers can use this information to further exploit the victim or sell it to other criminals.
- Use reputable vendors – Try to stick with legitimate and well-known vendors to avoid falling victim to a fraudulent website or company.

Unclassified//For Official Use Only

The information contained in this bulletin is For Official Use Only and is the property of the Commonwealth Fusion Center (CFC). It is intended for official use by law enforcement, public safety partners, and authorized critical infrastructure partners. No portion of this bulletin should be copied, released or re-disseminated without prior approval of the Commonwealth Fusion Center. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access. Information bearing the FOUO caveat may not be used in legal proceedings without first receiving authorization from the originating agency. Recipients are prohibited from posting FOUO information on a website or an unclassified network. Persons or organizations violating this policy will be prohibited from receiving CFC products.

- If uneasy about using certain websites, charitable donations, or smart device apps, try searching for online ratings and reviews. Victims of fraudulent or improper sites may leave reviews to warn others. Check for customer ratings and satisfaction before purchasing or sending money.
- Use secure websites – One way to make sure a website is safe is to look for the lock symbol () in the address bar. This shows that this website is using a secure network.
- Check bank statements regularly – Checking financial statements on a frequent basis will ensure that no financial accounts or information have been used without approval.
- Use credit cards over debit – If any fraudulent charges or purchases are made on a credit card, victims can contest them with their credit card company. Some debit cards do not have this same protection. Additionally, debit cards draw funds directly from a bank account, leaving a victim of theft with less actual currency to pay other bills.
- Never wire money or payment to a seller.
- Do not pay in pre-paid gift cards.
- Do not click links or download suspicious attachments from an email sender you do not recognize.
- Do not believe everything you see online.

(U) Response Considerations

(U) To report a suspected Internet-facilitated crime to the Federal Bureau of Investigation, please visit the FBI's Internet Crime Complaint Center (IC3):

(U) OUTLOOK

(U) The Commonwealth Fusion Center (CFC) Massachusetts Cybersecurity Program (MCP) is providing this information for situational awareness purposes only.

(U) Please report any suspicious activity to your police department of jurisdiction and the Commonwealth Fusion Center at 508-820-2233.

For additional information or to be added to the MCP distribution list, please contact the MCP by e-mail: MCPPOL@pol.state.ma.us.

This report addresses HSEC SINS: 1.1, 1.3, 1.8, 6
This report addresses CFC SINS: 1E, 1F

MSPC1989/MSPC1977

Sources:

- (U) "Holiday Scams – Shop Safely and Smarty online," Federal Bureau of Investigation, 1 December 2020
- (U) "FBI Warning: 'Tis the Season for Holiday Scams," Federal Bureau of Investigation, 23 November 2020
- (U) "'Tis the Season for Holiday Scams. Here's How to Spot Them and Avoid Them," Security National Bank, 20 November 2020
- (U) "Next Caller's 2020 Holiday Fraud Forecast: COVID-19 Primes Holiday Shopping Season For Massive Fraud," Next Caller, 13 October 2020
- (U) "Retail shrink tops \$50 billion as cyber threats become more of a priority," National Retail Federation, 6 June 2019
- (U) "Holiday shopping season 2020," Federal Trade Commission," 23 November 2020
- (U) "BBB Scam Alert: As holiday shopping fairs go virtual, scammers cash in," Better Business Bureau, 13 November 2020
- (U) "BBB Tip: Avoiding job scams this holiday season," Better Business Bureau," 6 November 2020
- (U) "BBB Tip: 5 top vacation scams to watch for when making travel plans," Better Business Bureau, 23 November 2020
- (U) "EI-ISAC Cybersecurity Spotlight – Typosquatting," Center for Internet Security, Accessed 7 December 2020
- (U) "Don't open it: Scam text message poses as package delivery notification," Fox 35 Orlando, 4 December 2020
- (U) "Is that text message about your FedEx package really a scam?" Federal Trade Commission, 20 February 2020
- (U) "The 15 Biggest Travel Scams, and How to Avoid Them," Smarter Travel, 26 September 2020
- (U) "BBB: Beware of online scams this holiday shopping season," CBS2 KUTV, 21 November 2020
- (U) "Don't post your travel plans on social media," Total Defense, accessed 10 December 2020

Unclassified//For Official Use Only

The information contained in this bulletin is For Official Use Only and is the property of the Commonwealth Fusion Center (CFC). It is intended for official use by law enforcement, public safety partners, and authorized critical infrastructure partners. No portion of this bulletin should be copied, released or re-disseminated without prior approval of the Commonwealth Fusion Center. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access. Information bearing the FOUO caveat may not be used in legal proceedings without first receiving authorization from the originating agency. Recipients are prohibited from posting FOUO information on a website or an unclassified network. Persons or organizations violating this policy will be prohibited from receiving CFC products.