As per Carbon Black threat report there is a 57.5% increase in attempted cyberattacks during the holiday shopping season (i.e. between US Thanksgiving through the New Year).

Cyberattacks are more prevalent during the holiday season

The excitement of the holiday season coupled with the volume of ecommerce and e-banking transactions provides ample opportunities for cyber-attacks. Cyber criminals take advantage of consumers and target rich environments such as financial institutions that rely on mobile technology as a payment platform to put themselves in a favorable position during the holidays.

Typically, at this time of the year hackers are looking to target individuals and organizations to steal money or financial information. They may also try to harvest sensitive details that can be used to steal a person's identity. Information such as social insurance numbers, addresses, drivers' licenses and credit union account information is very valuable to a cybercriminal.

Data breach, distributed denial of service attacks (DDoS), ransomware, spear – phishing and malware are some of the primary threats. Cyber criminals may deploy ransomware in financial institutions knowing that customer may need increase access to funds.

Red Flags

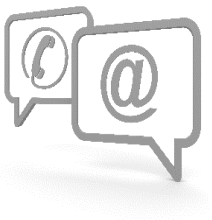
- A hacker may impersonate a senior staff member and send out spoof email to internal staff, members, vendors, to have fake invoices paid.
- Be skeptical of emails, messages or websites that contain misspelled common words or contain grammar errors. Email and web addresses should be examined for differences. For example, fedex.com might be changed to feddex.com
- Scammers may send text messages impersonating a financial institution typically asking the consumers to provide usernames, passwords, that can be used to commit financial crimes. For example, your credit union online access has temporarily been put on hold due to security verifications. Please confirm your account by signing in http://click-here.mobi/
- Everybody loves a great deal. But shocking offers, unbelievable discounts and unreal rates may signal that the offer isn't quite what it seems.

Preventions

The good news is that you can protect yourself from these types of cyber fraud by implementing a few basic measures in your daily online routines.

- One of the easiest and most important things you can do is to get in the habit of using strong password practices.
- Using Two-factor authentication (also known as 2FA or multi-factor authentication) provides an added layer of security for account access.
- You should never log into your online or mobile banking account while you are on a public computer or connected to public wi-fi. Public computers and wi-fi are regularly compromised by hackers. This easily allows them to steal your account credentials.
- If you receive that random e-mail from a reputable company, and they are asking for you to provide your sensitive information or credentials, be cautious, this may very well be a phishing e-mail. Legitimate organizations should never ask for your information by unsolicited e-mail.
- Never trust an email display name, always review and verify the actual e-mail address.
- Be cautious of any link or attachment provided in an e-mail.
- Check for spelling and grammar errors in the body of the e-mail.
- Check the salutation, you should be addressed by your name.
- Any requests for payment should be highly scrutinized and verified via telephone call (using number on file not in email) or in-person visit.
- Check the signature, a corporate signature should have business contact details.
- Don't click on any attachments.
- Be cautious of receiving a mail offer which guarantees you have won. Prizes might range from car to trips. If you have not entered a contest, it's probably a scam!

Finally, make sure you check your credit union account statement at least once a month. Look for unknown or suspicious account activity. If you see a transaction you don't recognize, immediately report it to your credit union.



For more information, please contact The CUMIS Risk Solutions Group at:
1-800-263-9120
Joel Grannum – joel.grannum@cumis.com / ext. 225053
Raksha Singh – raksha.singh@cumis.com / ext. 616059

Reference:

Carbon Black Holiday Threat Report 2018