CHRISTMAS

The most vulnerable time of the year!

At the end of a uniquely challenging year, Christmas will offer much-needed solace to many people. As with most major events since the start of the COVID-19 pandemic, however, it will feel markedly different as a result of ongoing social distancing restrictions. In particular, traditional gatherings and parties amongst colleagues, friends and family have largely been rendered impossible in many countries, while present shopping has significantly shifted online.

As a result, digital technologies will be relied upon like never before to enjoy the festive period, which unfortunately presents additional opportunities for cyber-criminals to launch attacks. Raef Meeuwise, CISM, CISA, author of Cybersecurity for Beginners, commented: “With many countries still taking considerable pandemic-related precautions, it’s beginning to look like a socially-distanced, virtual Christmas. That means more people shopping and sending things online, much to the delight of cyber-criminals.”

Rob Otto, EMEA field CTO at Ping Identity, added: “I think it’s inevitable that, as even more of our Christmas celebrations move online and virtual this year, attackers will become more active, simply due to the larger attack surface that is presented to them.”

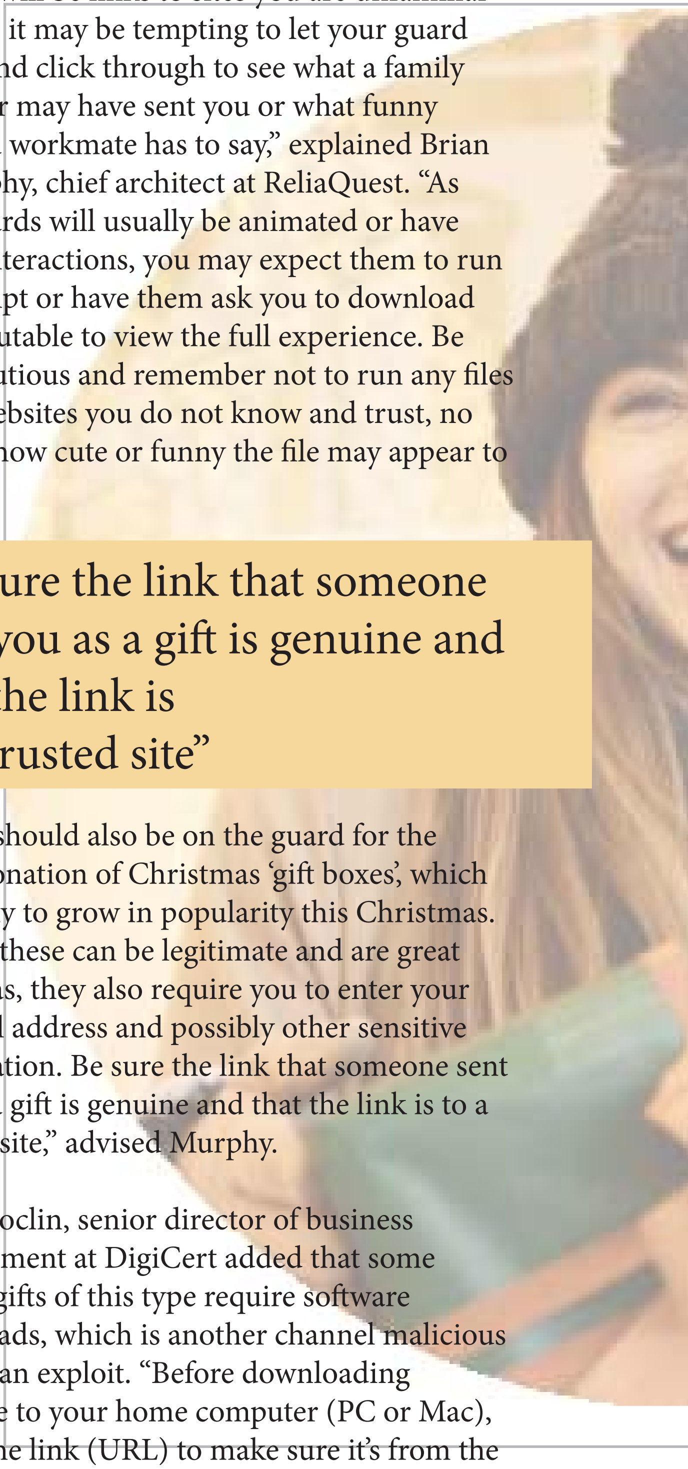
It is therefore crucial that amid the fun, relaxation (and perhaps odd alcoholic beverage), people are fully aware of the extra threats they will face this year and how to defend against them. Here are the top threats Infosecurity expects to see during this holiday season, and how they can be mitigated.

Seasonal Phishing Lures

The anxiety and fears brought about by the health, economic and social impact of COVID-19 have provided the perfect phishing lures to entice people into clicking on malicious links. The crisis has been heavily exploited by cyber-villains, with a huge increase observed in the number of phishing attempts this year via mediums such as email, social media and SMS.

Criminals have also regularly adapted the content of phishing messages according to evolving trends; for example, seizing upon the launch of government programs to support businesses and workers impacted by lockdowns. It is certain, therefore, that threat actors will exploit the virtual nature of Christmas 2020 to lure unsuspecting users to click on malicious links. Anthony James, VP of product marketing at Infoblox, stated: “A big concern is phishing, refreshed with timely holiday themes around charitable giving or gift giving to drive clicks to malicious sites.”

Virtual greeting cards may be heavily targeted by cyber-villains this year too, as remote friends and families seek to raise each other’s spirits through digital channels. “These, by their nature, will be links to sites you are unfamiliar with, so it may be tempting to let your guard down and click through to see what a family member may have sent you or what funny things a workmate has to say,” explained Brian P. Murphy, chief architect at ReliaQuest. “As these cards will usually be animated or have other interactions, you may expect them to run JavaScript or have them ask you to download an executable to view the full experience. Be very cautious and remember not to run any files from websites you do not know and trust, no matter how cute or funny the file may appear to be.”



> “Be sure the link that someone sent you as a gift is genuine and that the link is
> to a trusted site”

People should also be on the guard for the impersonation of Christmas ‘gift boxes’, which are likely to grow in popularity this Christmas. “While these can be legitimate and are great gift ideas, they also require you to enter your physical address and possibly other sensitive information. Be sure the link that someone sent you as a gift is genuine and that the link is to a trusted site,” advised Murphy.

Dean Coclin, senior director of business development at DigiCert added that some virtual gifts of this type require software downloads, which is another channel malicious actors can exploit. “Before downloading software to your home computer (PC or Mac), check the link (URL) to make sure it’s from the company you think it should be from. Also, when you download the code, a popup window will appear asking if you trust this software. This popup will normally have a link to the software author's identity. Click it to make sure it's from who you expect," he outlined.

Another potential phishing lure people should be particularly wary about are those relating to charitable donations, an area which has become increasingly important due to the economic impact of the crisis. Hank Schless, senior manager of security solutions at Lookout warned: "Threat actors could pose as charitable funds looking for donations around the holiday season. This is an easy way for them to steal your credit card information or have you deposit money directly into their account."

Online Christmas Shopping Lures

The pandemic has facilitated the rapid rise of e-commerce, which in turn has provided more opportunities than ever for fraudsters to strike. This includes a swathe of opportunities for phishing messages to be sent, ranging from fake discount offers to bogus delivery details, particularly during major shopping events such as Christmas. Otto highlighted: "With up to 30% of all Christmas shopping to be done online this year, consumers will find it hard to keep track of all the orders, delivery confirmations, payment approvals and so on, with the volume of such communications all within a short time window creating a lot of white space for cyber-criminals to exploit."

At a time of economic hardship for many, the temptation to click on links purporting to be bargain offers will be high. Meeuwisse said: "The rule as ever is that if something is too good to be true, it is probably a scam, especially if it is offering a cut-price, difficult to get hold of item (can I interest you in a PS5?) – with delivery before Christmas."

Meeuwisse added that delivery scams have been a growing area of concern this year, and again extreme caution should be exercised in relation to any correspondence of this nature. "A fully remote version of the scam just pretends to have an item to deliver to you and require some confirmation or a small payment before the item can be dispatched," he explained. "A more sinister version uses people on the ground who pretend to be delivery drivers and ask for a small payment (for example – because the parcel delivery cost was slightly underpaid) – and have a box of something unknown that requires a tiny payment using your credit or debit card. Once you make the payment – the scammer has your card details, PIN, address, name etc. and you have a box that turns out to have nothing of value in it. The driver is long gone once you make the payment."

As such, resisting any desire to immediately click on a link sent across is an important habit to get into. Coclin advised: "Before you click on the link, hover over it and see look at the URL to see where it's actually taking you. If it's a site you don't recognize, it's not necessarily bad but how can you tell? You can type the name of the site in a search engine to see what results come up or to see what others have to say about it. If you decide it's OK to go there, check the site's SSL certificate by clicking on the lock."

Securing Virtual Christmas Parties

The rapid move to remote working in at the start of COVID-19 in March brought about a surge in the use of video conferencing platforms as teams sought to stay connected. This was exploited by cyber-criminals, with numerous security vulnerabilities discovered on well-known platforms such as Zoom and MS Teams. While a big emphasis on improving the security on these platforms has been observed since, dangers remain for those who do not take sufficient precautions.

With physical parties out of the question in many areas of the planet, there is likely to be substantial use of video conferencing platforms to enable work colleagues, friends and family to celebrate Christmas remotely, and this is set to be targeted by cyber-criminals.

> “Treat your holiday parties like other meetings you have conducted throughout the year”

For organizations planning virtual Christmas parties, the same security protocols used for corporate meetings should not be relaxed. Sam Curry, chief security officer at Cybereason, noted: “Treat your holiday parties like other meetings you have conducted throughout the year. Continue to use waiting rooms, use unique codes, block recordings, have a published code of conduct, remind people to be on best behavior, etc.”

Tom Pendergast, chief learning officer at MediaPro, added: “This is NOT the time to experiment! Research the security and privacy policies of any tools you use to host a virtual party. You’ll want to ensure they meet your company’s infosecurity guidelines and that they respect your employee’s desire for privacy.”

It is highly likely a number of people will conduct Christmas gatherings with friends and family via their work laptops, meaning it is imperative for organizations to reiterate the most secure practices for organizing video calls to their employees. “To keep cyber-attackers at bay, it’s vital that organizations go beyond establishing baseline protocols to create and maintain a secure environment,” said Adam Philpott, EMEA president, McAfee.

In the view of Bill Santos, president and COO at Cerberus Sentinel, a good starting point for individuals arranging a virtual gathering is to use a platform that is well known and established. “Use a platform you are familiar with, especially the settings available to make a meeting private,” he advised.

Regardless of the conferencing platform used, the organizer should be familiar with its security settings, and be ready to take action if any issues emerge during the call. “By now, most people are familiar with Zoom, Webex and Teams, but there are similar platforms out there like Blue Jeans, Skype and Gotomeeting,” said Coclin. “If you are hosting on one of these, become familiar with the security settings so you don’t get ‘zoom bombed.’ These platforms have been enhanced with settings that allow you, as host, to screen entrants before they join, block/eject participants, implement permission based screen sharing and mute partakers."

Another thing people should be careful about is receiving links to virtual meet ups. Pendergast noted: "Scammers will try to spoof the more popular sites, so you'll want to verify that you've got the right download/URL."

This can be even harder to detect as particularly sophisticated cyber-criminals will have conducted research, enabling them to launch highly targeted and personalized messages, according to Schless. "Threat actors use sources such as social media profiles to learn more about individuals all the time. Oftentimes, we list our family on those profiles," he outlined. "An attacker could pose as a family member and send malicious links masked as video call invites, tracking information for presents or fun online games that bring families together."

Targeting Christmas Apps/Games

During the course of virtual gatherings of friends and family, it is certain virtual quizzes and other games will be downloaded and played by participants. Many will come from the various holiday-themed games apps and activities that can be downloaded on phones and other devices, which provides yet more opportunities for cyber-criminals to launch attacks. "There could be an uptick in malicious versions of legitimate holiday-themed apps. It's common for malicious actors to break down an app, add malware to it, then redistribute it outside legitimate app stores through social media, SMS campaigns or third-party app stores," outlined Schless.

Javvad Malik, security awareness advocate at KnowBe4, added: "With a virtual Christmas expected this year, it is likely that many people will look at online games or other virtual apps to connect the family. However, criminals will also look to exploit these, either by releasing apps of their own, or finding ways to gain access to apps which are poorly secured or misconfigured."

As is the case with arranging virtual meet ups, people should ensure they know the app is genuine before downloading even if it is available on a legitimate app store, as well as maintaining basic security hygiene. "It is best to stick with known and trusted apps, but even with these apps, it is important to set the right controls to ensure no unauthorized people can join and a strong password is used," advised Malik.

Christmas 2020 will sadly consist of far less physical social gatherings, although a saving grace is that advances in digital technology will at least partially replicate some of the enjoyment and socializing among friends and family. It is important that people remain vigilant when doing so, however, due to the increased opportunities that the growing use of online shopping and virtual gatherings will present to malicious actors. Awareness of the types of tactics cyber-criminals will employ, along with basic security steps that can be taken to mitigate them, can help prevent Christmas being the most vulnerable time of the year.

Happy
Safe
Holidays!