HOT SUMMER CYBER SCAMS

June 2023| Issue 2023:4

THE SOCIAL SIDE OF SUMMER SCAMS

Summer for many is prime travel and vacation time. We're often excited about planning our trips and anxious to get the best prices and accommodations. Cybercriminals are aware of this and use a number of ploys to steal data and information, many of which are based in social engineering.

Crowdstrike defines social engineering as a cybersecurity attack that relies on the psychological manipulation of human behavior to disclose sensitive data, share credentials, grant access to a personal device or otherwise compromise their digital security.

Social engineering attacks pose a great threat to cybersecurity since many attacks begin on a personal level and rely on human error to advance the attack path. By invoking empathy, fear and urgency in the victim, adversaries are often able to gain access to personal information.

One of the greatest dangers of social engineering is that the attacks don't have to work against everyone: A single successfully fooled victim can provide enough information to trigger an attack that can affect an entire organization.

Over time, social engineering attacks have grown increasingly sophisticated. Not only do fake websites or emails look realistic enough to fool victims into revealing data that can be used for identity theft, but social engineering has also become one of the most common ways for attackers to breach an organization's initial defenses in order to cause further disruption and harm.

While it is impossible to prevent social engineering attacks from taking place, people and organizations can protect themselves through responsible behavior, security awareness, education and vigilance. Delaware's state government recognizes the value of continuing cybersecurity awareness and training for all network users.

We value the input of our network users and those of you who take the time to read this monthly newsletter. **We encourage you to share your thoughts on the latest cybersecurity trends and challenges**. What topics would you like to see covered in our upcoming issues? Do you have any personal experiences or insights to share? Please email us your feedback and suggestions. We look forward to hearing from you!

Solomon Adote
Chief Security Officer

DON'T LET SCAMMERS RUIN YOUR VACATION

Summer is a time for relaxation, vacation and fun. But it can also be a time for cybercriminals to target unsuspecting people with scams and frauds. Whether you are planning to travel, shop online or use public Wi-Fi, you need to be aware of the potential risks and how to protect yourself from falling victim to cyberattacks.

Vacation Lodging

Cyberthieves are finding new ways to fleece unwitting travelers. More than half of vacationers say they are likely to use the internet to search for travel bargains in light of inflation, with over a third saying they are more likely to use booking sites they haven't used before in order to find a good price. Scammers may post fake listings of vacation properties on social media or online platforms and ask you to pay upfront or provide your credit card information. You may end up losing your money or arriving at a non-existent or already occupied property.

Being aware and doing some research first will help you to establish the legitimacy of your rental choice. Be on alert for any rental that insists payment by cryptocurrency, gift cards or wire transfers. Check that the address of the property really exists. If the property is located in a resort, call the front desk and confirm their location and other details on the contract.

Hotels

There are several scams that can happen when using hotel Wi-Fi. The FBI warns that Wi-Fi networks in hotels typically favor guest convenience over strong security practices. This means that hotel Wi-Fi is designed for easy access, which can make it vulnerable to cyberattacks or scams.

Free Wi-Fi is a doorway for scammers, but not everyone realizes it. Scammers can set up fake Wi-Fi hotspots with names similar to the hotel's network name. When you connect to these fake hotspots, scammers can steal your personal information.

NordVPN recommends that to avoid being hacked through hotel Wi-Fi, travelers should ask the person at the reception desk to give the exact name and password for the provided Wi-Fi to avoid connecting to a fake network. Keeping the automatic connection function disabled on your devices helps to mitigate risks on a trip because devices may be surrounded by public and insecure internet connections.

Smart TV Cyber Stalking

A smart TV can be another gateway for cybercriminals. The televisions have an established connection to local Wi-Fi allowing travelers to access apps and streaming platforms.

A hacked smart TV could be used for cyberstalking visitors with built-in microphones or cameras, or stealing personal credentials used to log in to apps on smart TV and selling them on the dark web.

The best thing to do according to Nord VPN is to keep the smart TV unplugged from power sources when it's not being used. Covering the webcam and avoiding logging in with personal credentials also mitigates cyber risks.

READ MORE CYBERSECURITY NEWS at DIGIKNOW!