Stay Safe Online: Understanding Cyber Risks This Holiday Season

By Kenneth Hizon, Guam SBDC Business Advisor
October 1, 2024

The holiday season is a time for fun, shopping, and connecting with loved ones. But it's also a time when cybercriminals try to take advantage of our increased online activity. Here's what you need to know to keep your personal and financial information safe.

Why Cyber Attacks Rise During the Holidays

- **Increased Online Transactions:** With shoppers taking advantage of online deals and discounts, there is a significant rise in digital transactions. This provides cybercriminals with ample opportunities to intercept financial data.
- **Distraction and Multitasking:** Amidst the busy schedules of holiday planning and shopping, individuals are more distracted and may not scrutinize online interactions diligently, making them more susceptible to scams.
- **Targeted Businesses:** Retailers and e-commerce platforms, which see a spike in sales during this period, are prime targets as attackers attempt to hack into systems to steal customer data or disrupt operations, sometimes holding systems for ransom.
- **Generosity Exploitation:** The spirit of giving during the festive season is often manipulated by fraudsters setting up fake charities or donation platforms to solicit funds that never reach those in need.

Main Cyber Threats to Watch Out For

- **Payment Card Skimming:** Cybercriminals deploy skimming tools on compromised websites to capture credit card information during online transactions without the user's knowledge.
- **Gift Card Scams:** Scammers trick individuals into purchasing gift cards as a form of payment or as part of a fake promotion. Once the scammer has the gift card number and PIN, the funds are quickly drained.
- **E-Greeting Card Scams:** Fake e-greeting cards contain links or attachments that, when clicked or downloaded, install malware or lead to phishing sites designed to steal information.

- **Travel Scams:** During the holidays, many people make travel arrangements, which scammers exploit by setting up fake travel sites or sending phishing emails offering unbelievable travel deals.
- **Package Delivery Scams:** As deliveries increase during the holiday season, scammers send fake notifications that appear to be from legitimate delivery services, prompting users to click on links leading to malicious sites.
- **Social Media Scams:** Fraudsters create fake social media ads or posts offering deep discounts, free gifts, or contests requiring personal information, which they then use for malicious purposes.
- **Phishing Scams:** Beware of emails and messages that seem legitimate but contain malicious links or attachments. These often appear to be from trusted retailers or friends offering holiday deals or promotions. Always verify the sender before clicking on any links.
- **Fake Online Stores:** Some websites offer deals that are too good to be true, designed solely to capture your payment information. Always shop from reputable stores, and check reviews or ratings before purchasing from unfamiliar sites.
- **Malware and Ransomware:** Be mindful of what you click on—some files or advertisements can download malware onto your device. This can not only disrupt your personal files but also demand a ransom for their release.
- **Insecure Wi-Fi Networks:** Many people travel during the holidays and rely on public Wi-Fi, which can be insecure. Hackers can easily intercept data sent over unsecured networks or set up fake Wi-Fi hotspots to capture information.

What Cybercriminals Want

- **Personal Information**: For identity theft or creating fake accounts.
- **Financial Information**: Credit card numbers and bank details can be used for theft or sold online.
- **Login Details**: Reused passwords can give access to many accounts.
- **Business Disruption**: Cyber attacks on businesses can lead to ransom demands.

How to Protect Yourself

- **Verify Email and Message Sources:** Before clicking on any links or opening attachments, check the sender's identity and look for any unusual language or request that could indicate a phishing attempt.

- **Shop on Secure, Reputable Websites:** Stick to trusted retailers and ensure the website address starts with "https://", indicating a secure connection. Review privacy policies and customer reviews where possible.
- **Use Strong, Unique Passwords:** Utilize complex passwords and a password manager. Ensure two-factor authentication is enabled for added security on all accounts where available.
- **Stay Educated:** Keep informed about the latest cyber threats and share this information with loved ones to enhance collective vigilance.
- **Regular Software Updates:** Always update your devices and security software to protect against vulnerabilities that hackers could exploit.

By staying alert and informed, you can enjoy the holiday season without falling victim to cybercriminals. Ensuring your online safety means you can celebrate with peace of mind.