Protect Your Assets From Identity Thieves

Identity thieves and cyber criminals are relentless in their pursuit of personal information, and in some cases, financial assets. Total combined fraud losses reached $56 billion in 2020, with identity fraud scams accounting for $43 billion and traditional identity fraud losses totaling $13 billion.* Through education and good cyber security practices, you can significantly reduce the risk of becoming a victim of fraud and cybercrime.

During the holiday season, cybercrime activity triples. Fake package delivery e-mails, retailer notifications, and e-cards are just a few tactics that criminals employ. Here are some other things to be aware of to keep your personal information safe.

Don't Get Hooked by Phishing. Don't carelessly open attachments or click on hyperlinks in e-mails. Viruses, ransomware, and password theft could be one wrong click away.

Passwords Are the Key to Your Information and Assets. Always protect your financial account, e-mail, computer, and social media passwords. Don't share or provide a password over the phone or through a link you receive in an e-mail. No financial services or IT professional will ever have a legitimate reason to ask for your password.

Be Mindful of Social Engineering Attempts. Cyber criminals rely on fear, hope, and trust. Phone calls and e-mails with a sense of urgency, legal threats, or incredible offers are a few tactics used to get your personal information or money. Don't trust unsolicited phone calls or e-mails asking for payment or personal information.

Public Wi-Fi Is a Hunting Ground for Cyber Criminals. You might think you are connecting to a legitimate and safe public Wi-Fi network. Criminals can easily spoof these networks and intercept your information. Your passwords, e-mails, and personal information are all at risk. If you must connect to public Wi-Fi through your phone or computer, consider using a virtual private network (VPN) service.

* Source: Javelin Strategy & Research 2021 Identity Fraud Study

STIFEL