SONTIQ

EZShield IdentityForce

6 TIPS TO STAY SAFE & CONNECTED DURING THE HOLIDAYS

1. **Secure Your Online Video Platforms** | Hosting a Zoom dinner for the holidays? Before accepting invitations or creating meetings on a video conferencing app, check security settings and ensure the meeting is encrypted and private. Video conferencing has been a fast-growing hacker target since the COVID-19 pandemic ushered in social distancing and closed schools and office buildings across the country. Unsafe video chats, conferencing software, and bogus online meeting login websites may leave your family vulnerable to malware or unwanted visitors.

2. **Safeguard Your Devices** | Planning to live-stream over social media, or direct video connections via smart device while doing meal prep or gift exchanges? Desktops and laptops should have anti-virus and online PC security tools that keep your activity shielded from hackers while shopping, banking, or sharing online. Mobile devices need protection, too, so invest in mobile security that alerts you of rogue applications, spyware, and unsecured Wi-Fi connections, and even better if it includes a Virtual Private Network (VPN) for safer Wi-Fi connections.

3. **Update Your Passwords** | Account security is a growing concern, as billions of login credentials are circulating on the Dark Web, and millions are being given away for free. Exposed usernames and passwords can give hackers access to your personal and financial information through credential stu ing attacks, opening the door to account takeover fraud. Be sure to update your passwords regularly, creating unique, strong sequences every time — and don't reuse passwords across personal and business accounts.

4. **Beware of Scams Targeting Kids** | Children have been online more than ever this year, learning, playing, and socializing, and the holidays will be no different. Scammers will keep trying to obtain their personal information through online tricks. Children's Social Security numbers, unused credit histories, and even health insurance information, are a gold mine for cyber thieves because they can sell it on the Dark Web for large profits, or use it themselves without fear of getting caught for many, many years.

5. **Take Charge of What You Share** | Control how much personal information you and your family make available online, as it can provide the type of information used in imposter scams and social engineering scams against you, or your friends and family. Teach children to avoid oversharing, especially on social media and online gaming platforms. Also, take note of who sees your posts and profile information by updating account settings on each social platform. Get a helping hand protecting yourself and your children with social media identity monitoring to detect inappropriate activity and posts that may be perceived as violent, use profanity, or are indicative of cyberbullying.

6. **Beware of Social Media Ads** | November often kicks off amazing holiday discounts, major increases in online shopping, and personal distractions galore. Be wary of social media posts and ads that appear on your social newsfeeds, especially in the year of coronavirus. They could be part of a phishing attack that redirects you to a fraudulent website in order to steal your personal or financial information. Or, a malware scheme using hacked social accounts, posting ads designed to hold your device data for ransom. Be sure to use two-factor authentication (2FA) on all your accounts to keep hackers out.

ABOUT SONTIQ

Sontiq is an intelligent identity security company arming businesses and consumers with award-winning products built to protect what matters most. Sontiq's brands, EZShield and IdentityForce, provide a full range of identity monitoring, restoration, and response products and services that empower customers to be less vulnerable to the financial and emotional consequences of identity theft and cybercrimes. Learn more at www.sontiq.com or engage with us on Twitter, Facebook, LinkedIn, or YouTube.