# DEFENDING YOUR DIGITAL CHIMNEY

SLEIGH YOUR CYBER

WITH TRAVA

## KEEPING CYBER GRINCHES AT BAY

'Tis the season to be jolly, but it's also the season when cyber grinches are lurking in the digital shadows, ready to steal your festive joy. To ensure your holiday season is full of cheer and your online experiences are as safe as possible, we've unwrapped a set of cybersecurity tips that will keep you and your loved ones secure as you surf the winter wonderland of the internet.

- **Use Strong and Unique Passwords**
  Ensure that you have strong, unique passwords for all your online accounts. Consider using a password manager to generate and store complex passwords securely.

- **Enable Multi-Factor Authentication (MFA)**
  Enable MFA for your accounts. This adds an extra layer of security by requiring you to provide a second verification, such as a code sent to your phone, as well as your password.

- **Beware of Phishing Scams**
  Be cautious about clicking on links or opening email attachments, especially if they are unsolicited or appear to be from unfamiliar sources. Cybercriminals often send phishing emails during the holiday season.

- **Shop from Reputable Websites**
  When shopping online, only use trusted and well-known websites. Look for "https://" in the website's URL and a padlock symbol in the address bar, which indicates a secure connection.

- **Be Careful with Public WiFi**
  Avoid using public WiFi networks for sensitive activities like online shopping or banking. If you must use public WiFi, consider using a VPN to encrypt your connection.

- **Update Software and Devices**
  Keep your operating system, antivirus software, and applications up to date with the latest security patches. Cybercriminals often target known vulnerabilities.

- **Be Cautious on Social Media**
  Avoid oversharing personal information on social media, as cybercriminals can use this information for social engineering attacks. Also, be wary of friend requests or messages from unfamiliar individuals.
- **Check Your Financial Statements**
  Regularly review your credit card and bank statements for any unauthorized transactions. If you spot any discrepancies, report them immediately.
- **Secure Your Home Network**
  Make sure your home WiFi network is secure by using a strong, unique password and enabling WPA3 (Wi-Fi Protected Access 3) encryption. Change default router login credentials.
- **Backup Your Data**
  Regularly back up important data to an external drive or a secure cloud storage service. This can help you recover your data in case of a cyberattack or data loss.
- **Be Wary of Gift Card Scams**
  Be cautious if someone asks you to purchase gift cards for them, especially if it's done through unsolicited phone calls or emails. Scammers often use this tactic.
- **Use Secure Payment Methods**
  When making online purchases, use secure payment methods like credit cards, which typically offer more protection than debit cards or wire transfers.
- **Install Security Software**
  Use reputable antivirus and anti-malware software on your devices to help detect and prevent threats.
- **Stay Informed**
  Stay up to date with the latest cybersecurity news and threats to be aware of new tactics and scams.

**BY FOLLOWING THESE TIPS, YOU CAN SIGNIFICANTLY REDUCE THE RISK OF FALLING VICTIM TO CYBERATTACKS DURING THE HOLIDAY SEASON AND ENSURE A SAFER ONLINE EXPERIENCE FOR YOURSELF AND YOUR FAMILY.**

Your cybersecurity needs are unique and require unique solutions. **Schedule a demo today!**

talk to trava

TRAVA
Stellar product.
**Better people.**