KEEP YOUR HOLIDAYS *Merry*

FOLLOW THESE TIPS TO PROTECT YOURSELF

TIP #1 UPDATE YOUR ANTI-VIRUS SOFTWARE

The holidays are upon us, but before you get into holiday shopper mode, make sure your anti-virus software is up to date – it's the best way to protect your computer (and your data) from malware. Same goes for mobile anti-virus software for your smartphone.

TIP #2 CREDIT CARDS vs. DEBIT CARDS

Credit cards have advantages over debit cards when it comes to security, but many prefer to stick with their debit card for holiday shopping to avoid high credit card bills.

TIP #3 DON'T BE FOOLED BY LOW PRICES

If the deal seems too good to be true, it probably is. Criminals lure shoppers with websites that look legitimate and offer unbelievably low prices in an effort to capture your personal information.

TIP #4 STAY ALERT

Distracted shoppers make easier targets for criminals. As you're doing your holiday shopping, be aware of your surroundings, park in well-lit areas and put away your phone to keep your hands free. Additionally, don't leave your wallet, purse, phone, packages or other valuables in your vehicle.

TIP #5 STAY SAFE SHOPPING ONLINE

Be sure to look for the closed lock icon to the left of the web address in your browser window, and make sure the web address begins with "https"— the "s" means it's secure. Holiday shopping makes consumers especially vulnerable to identity theft – that's why December is National Identity Theft Prevention and Awareness Month.

TIP #6 DON'T USE PUBLIC USB CHARGING STATIONS

As you travel for the holidays, beware of "juice jacking." It's a scheme where public USB ports are hacked to install data-stealing malware onto your phone. This allows criminals to access information from personal passwords and bank accounts to entire backups of your phone. Instead of using USB charging stations, plan ahead and bring an AC charger or portable battery.

TIP #7 BEWARE OF FAKE DELIVERY ALERTS

As you await delivery of holiday packages, be aware of fraudulent shipping notices that look like they're from known carriers like FedEx, UPS or the US Postal Service. Criminals often send deceptive emails with a link to a fake delivery alert which, if clicked, can download malware to your computer or mobile device. Be sure you only use the tracking numbers provided in the confirmation email from your online purchase.

TIP #8 MONITOR YOUR ACCOUNTS REGULARLY

Even if your holiday shopping may be wrapping up, that doesn't mean fraudulent activity is over. We urge you to set up online banking and mobile banking to monitor your accounts regularly (and year-round) for fraudulent activity.

TIP #9 BEWARE OF CHARITY SCAMS

The end of the year is a popular time for charitable donations. Avoid scammers and not-so-reputable charities by only giving to charities that you know well. Phony charities use names that sound like real ones. Scan the QR Code or visit www.CharityNavigator.org to confirm the nonprofit's exact name on their site.

COMMUNITY FIRST BANK

We know what matters.

C1stBank.com