PCS
4th Quarter
Newsletter
2020

5 Safe Online Shopping Tips

During this 2020 season of giving amidst the uncertainty surrounding the global pandemic, the numbers of holiday shoppers making purchases online will continue to rise. According to Deloitte's annual holiday retail forecast predictions, e-commerce sales will grow by 25-35% over 2019, generating between $182—$196 billion this holiday season.

Unfortunately, it's also the season for online scammers to make a killing—typically at your expense. Online purchase scams, which can expose your identity and even drain your wallet, are the riskiest form of consumer fraud, according to a report published by the BBB (Better Business Bureau). A recent Experian survey found 43% of victims said their identity theft occurred while holiday shopping online.

The holidays should be a time of joy as you spend time with friends and family—not stress and frustration as you untangle a case of identity theft or financial fraud. Stay ahead of online scammers and identity thieves by using these tips on the following page to help secure your personal information while shopping online.

Pittsburgh Computer Solutions

Safe Online Shopping Tips Continued

1. Ship to a secure location. The rise of online shopping has led to an increase of home deliveries — and with it, an increase in “porch pirates”, or thieves who steal packages from doorsteps. If no one’s home to accept a package, consider shipping to your office or another safe place. UPS, Amazon, and FedEx all now have shipping lockers available for secure deliveries.

2. Never make purchases on public Wi-Fi. You might be tempted to take your shopping spree to a coffee shop for a cup of joe. Keep in mind, Wi-Fi networks use public airwaves. With a little tech know-how and the freely available Wi-Fi password at your favorite cafe, someone can intercept the data you send and receive while on free public Wi-Fi. Shopping online usually means giving out information that an identity thief would love to grab, including your name, address, and credit card information. Bottom line: It’s never a good idea to shop online or log in to any website while you’re connected to public Wi-Fi.

3. Don’t get tripped up in holiday shopping scam emails. Sometimes, something in your email in-box can stir your holiday consumer cravings. For instance, it might be tempting to open an email from an unfamiliar business that promises a “special offer.” But that offer could be special in a bad way. Clicking on email from unknown senders and unrecognizable sellers could infect your computer with viruses and malware, or lead you to a false site developed to steal your data. Delete them, don’t click on any links, and don’t open any attachments from individuals or businesses you are unfamiliar with.

4. Always use strong passwords. If someone has the password to your account, they could log in, change the shipping address, and order things with stored payment data while you get stuck with the bill. Help keep your account safe by securing it with a strong password—”Santa123” won’t do. Here are some tips on how:

- Use a complex set of at least 10 lowercase and uppercase numbers, letters, and symbols.
- Don’t use personal information that others can find or guess, such as birthdates, your kids’ names, or favorite color.
- Don’t use the same password—however strong—on multiple accounts. A data breach at one company could give criminals access to your other, shared-password accounts.

5. Try shopping with the extra security of a VPN. Still can’t resist the lure of shopping online while sipping that peppermint latte? If you must shop online on public Wi-Fi, consider installing and using a VPN — short for virtual private network — on all mobile devices and computers before connecting to any Wi-Fi network. A VPN creates an encrypted connection between your smartphones and computers and the VPN server. Think of it as a secure tunnel your Internet traffic travels through while you browse the web, making the data you send and receive safer from interception by nearby hackers. Follow these online shopping tips not only for the holidays but all year round.

How to Remember Where You Parked Using the Google Assistant

There's nothing quite like the frustration of forgetting where you parked. You can tell how common this problem is by the multitude of solutions available. The best is the one that requires very little effort. As long as you have Google Assistant on your Android device, iPhone, or iPad, and you have it with you when you park, this method will work and you can quickly find your vehicle!

Google Assistant for Android

The first thing you have to do on your Android device is make sure Google Assistant can access your location. Make sure "Use Location" is toggled On.

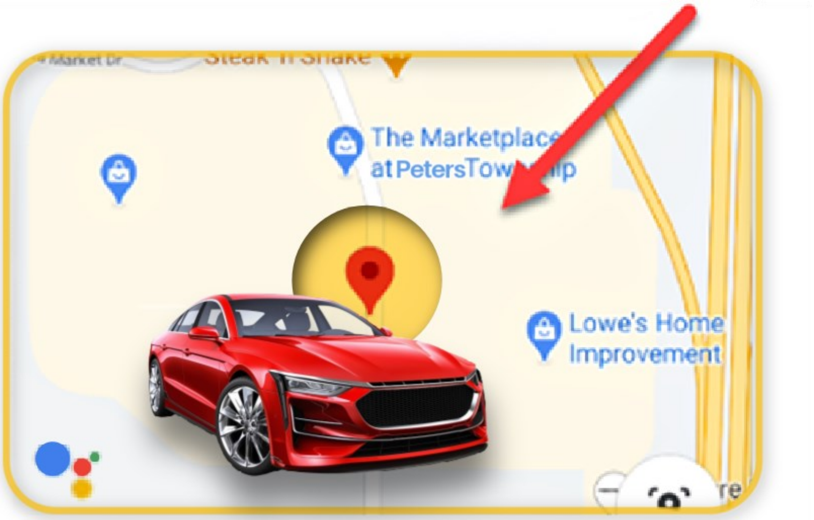
Once that's out of the way, you can now use the parking feature. The first thing you have to do is open Google Assistant in one of the following ways:
Say "Okay Google" or "Hey Google." When Google Assistant is listening, you can say one of the following commands:

- "I parked here."
- "Remember where I parked."

Google Assistant will save your parking location on a map.

When you're ready to return to your vehicle, open the "Google Assistant" again. Then, say any of the following commands:

- "Where's my car?
- "Where did I park?"
- "Find my car's location"



A map will appear showing you where your car is parked; tap it to open it in Google Maps and navigate to your parking spot. Google saves your parking location for 24 hours. If you want to remove it sooner, just say, "Forget where I parked." to Google Assistant. Google Assistant then responds with "Done. It's forgotten." As easy as that!

This works for iPhones and iPads as well.

make your workplace more secure
with 2-factor authentication

With so much of our lives happening on mobile devices and laptops, it’s no wonder our digital accounts have become a magnet for criminals. Malicious attacks against governments, companies, and individuals are more and more common. There are no signs that the hacks, data breaches, and other forms of cybercrime are slowing down.

For most organizations, apps, programs and systems, using a username and password is how they authenticate users. According to a recent report, stolen, reused, and weak passwords remain a leading cause of security breaches. Unfortunately, passwords are still the main (or only) way many companies protect their users. One way to quickly boost the safety of your online accounts is two-factor authentication (2FA) which adds an extra layer of security to your accounts

What is two-factor authentication (2FA)?

Two-factor authentication (2FA) is an extra step added to the log-in process, such as a code sent to your phone or a fingerprint scan, that helps verify your identity and prevent cybercriminals from accessing your private information. 2FA offers an extra level of security that cyberthieves can’t easily access, because the criminal needs more than just your username and password credentials.

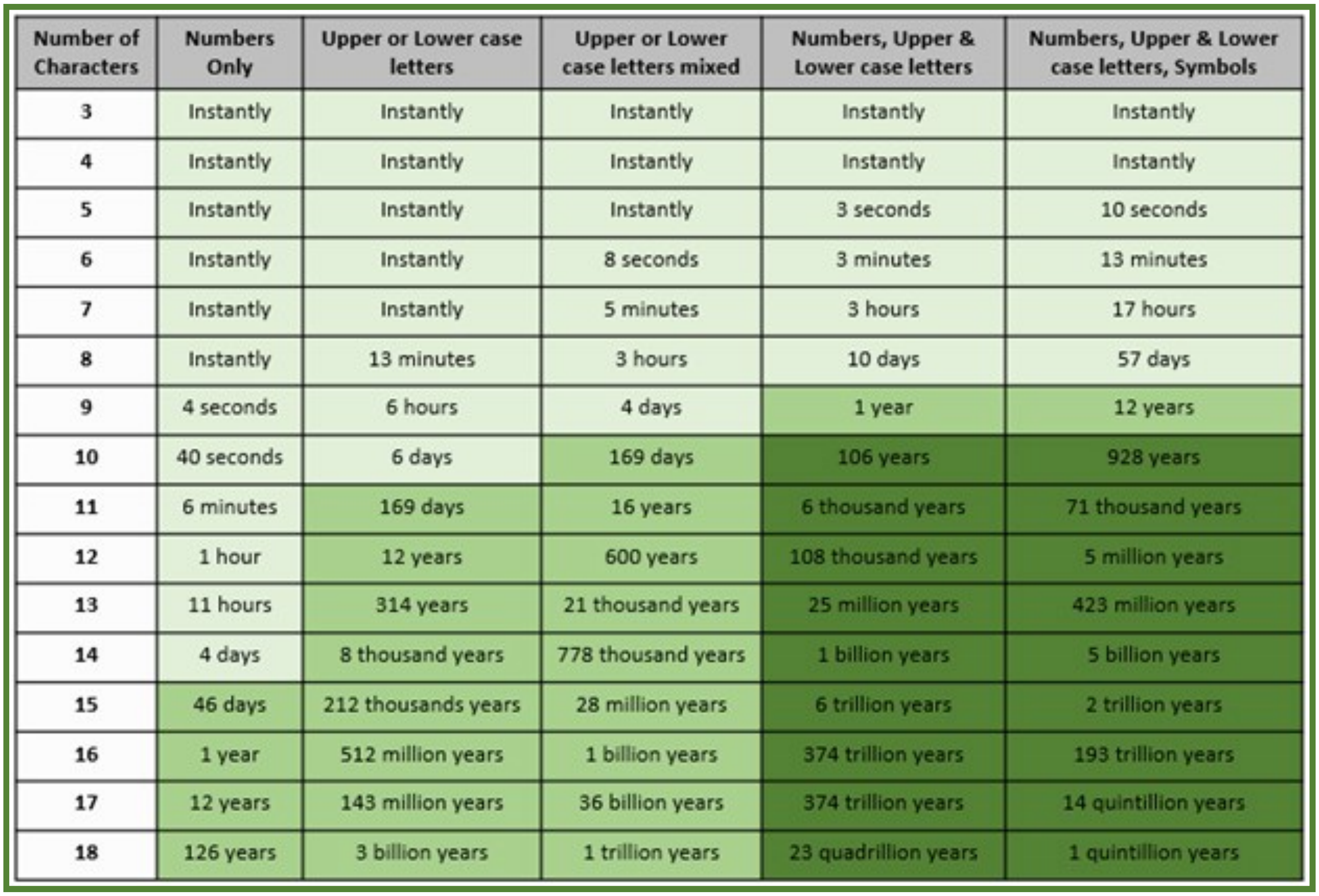
As the name suggests, two-factor authentication requires one extra step — and a second factor — to log onto a site or access an online account. Most often, you first enter your username and password. The site typically then sends a text message to your mobile phone with a six-digit numerical code. This code is called an authenticator, or sometimes a passcode or verification code. You can only access the site by then entering this code that appears on your mobile device. If you don't have the code, you can't log on, even if you know the correct password.

Google Authenticator is a software-based authenticator by Google that implements two-step verification services. Authenticator generates a six-to eight-digit one-time password which users must enter in addition to their usual login details. To use Authenticator, the app is first installed on a smartphone. It must be set up for each site with which it is to used, the site provides a shared secret key to the user over a secure channel, to be stored in the Authenticator App. This secret key will be used for all future logins to the site.

To log into a site or service that uses two-factor authentication and supports Authenticator, the user provides username and password to the site, which computes (but does not display) the required six-digit one-time password and asks the user to enter it. The user runs the Authenticator app, which independently computes and displays the same password, which the user types in, authenticating their identity.

With this kind of two-factor authentication, mere knowledge of username and password is not sufficient to break into a user's account, the attacker also needs knowledge of the shared secret key, or physical access to the device running the Authenticator app.

Simply put dual factor authentication lowers a company's risk of a data breach. If your business needs some guidance on enabling two-factor authentication, please contact PCS. We can help you to assess the best methods to increase security for your systems and networks.



Number of Characters	Numbers Only	Upper or Lower case letters	Upper or Lower case letters mixed	Numbers, Upper & Lower case letters	Numbers, Upper & Lower case letters, Symbols
3	Instantly	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	3 seconds	10 seconds
6	Instantly	Instantly	8 seconds	3 minutes	13 minutes
7	Instantly	Instantly	5 minutes	3 hours	17 hours
8	Instantly	13 minutes	3 hours	10 days	57 days
9	4 seconds	6 hours	4 days	1 year	12 years
10	40 seconds	6 days	169 days	106 years	928 years
11	6 minutes	169 days	16 years	6 thousand years	71 thousand years
12	1 hour	12 years	600 years	108 thousand years	5 million years
13	11 hours	314 years	21 thousand years	25 million years	423 million years
14	4 days	8 thousand years	778 thousand years	1 billion years	5 billion years
15	46 days	212 thousands years	28 million years	6 trillion years	2 trillion years
16	1 year	512 million years	1 billion years	374 trillion years	193 trillion years
17	12 years	143 million years	36 billion years	374 trillion years	14 quintillion years
18	126 years	3 billion years	1 trillion years	23 quadrillion years	1 quintillion years

Ever wonder just how easy it is for someone with ill intent to crack your password using a computer program? The above table demonstrates the correlation between password strength and the potential time it can take to crack using a specialized computer program.

datto | SIRIS

Your business is at risk every day. Simple daily backups are not enough to ensure your business can keep running in the event of ransomware attacks, natural disasters, equipment failure, and human error. If disaster strikes, how will you ensure that your technology has enough flexibility, redundancy, and resilience to protect your data while remaining simple to set up, use, and recover? Datto SIRIS is the all-in-one total data protection solution built to efficiently prevent data loss and minimize downtime.

Backup and restore critical business data, keep your business running during a disaster, locally or from the Datto cloud. Protect against ransomware threats before they impact you business. When disaster strikes your business there is no time to waste. Waiting on outdated and unreliable technology to restore backups can significantly impact the business.

With Instant Virtualization, your business can restore within seconds from their local device or using Datto's powerful cloud. While a complete image of your system runs through a virtual machine, regular backups continue. And if you lose the entire source machine, SIRIS also provides the option for bare metal restore into new hardware or a virtual destination.

Detect ransomware threats before they happen. SIRIS monitors and targets specific patterns of ransomware within a single backup, notifies you, and helps you get back to business without paying ransom.

Companies can't count on unreliable, outdated backup methods that take too long to restore files and have a high risk of losing data to corruption. Datto gives you the power to protect critical data and keep your business running during a disaster, all in a single solution supported by a world class, 24/7, 365 tech support group. Rest easy knowing your data is protected and your business can run anywhere.

Pittsburgh Computer Solutions offers a range of Datto backup and business continuity solutions for companies of all sizes.

We provide a combination of on - premises, virtual, and cloud-to-cloud data protection. We'll provide a solution that meets your needs and fits your budget.

Protect your business data!
Call PCS today at 724-942-1337.