10 Most Common IT Questions

By Client Tech

1. Do I really need to change my password often?

The answer to this is simple: yes. Changing your password regularly limits account breachers, prevents leaks, and protects your private information. Whether it's your email, social media, online bill pay or online banking software, changing your password regularly helps protect you from unwanted scams, hacks, and potential data loss.

2. Are my files safe if I upload them to online websites?

While some websites are safe, there are many websites that simply aren't. Just recently, all images and data that was stored on Myspace.com were lost. While many people still used Myspace.com as a way of storing old memories, they didn't think to export the images and save them to a more reliable database, like a cloud software.

3. Why is there a need for IT? Aren't bots just sci-fi related?

Every day, we work diligently to ensure that the technology you rely on to run your business is secure, up to date, running smoothly and helping you succeed. In a perfect world that would mean that no server ever crashed, no virus ever downloaded, and no hardware ever failed. But, these things happen. Bots, though by the sound of the word, sound much like a sci-fi drama, are actual real threats in the business and personal world of the internet. Malicious bots can cause a lot of damage to data and files and often steal passwords, obtain financial information, launch DoS attacks, open back doors on an infected computer and other harmful things that are detrimental.

4. What is the Cloud? How does it work?

When you hear that your data or photos are stored on the cloud, tech professionals aren't referring to the white clouds in the sky. Instead, they're referring to software run on the internet, rather than your computer, that hosts data. Cloud services include Google Drive, Apple iCloud, Dropbox and Microsoft OneDrive. The benefits of storing your files on the cloud allow for easy access across all devices granted you have access to the internet.

5. Can Facebook polls and quizzes hack my computer and/or files?

Recently, Facebook users across the world are taking part in fun, quirky Facebook games and polls. For the game to compute an answer, it asks various questions like: What's your favorite color? Where did you grow up? What's your Mother's maiden name? Where did you go to high school?

While it seems completely innocent, giving possible hackers answers to personal questions opens the doors for hackers and digital threats to take place.

6. Does it matter who buys my domain name?

Absolutely. When you purchase a domain for a new or existing website, it is important that a business owner or partner handle the domain information. Often times, a non-essential employee buys the domain for the company, and when the employee is no longer with the company, the company loses access to the domain login and additional information that is needed to make updates and ensure the website is online.

7. When traveling, is it safe to use my phone?

When traveling, it's important to be aware of public wifi. In addition, it's important to use apps that are safe and reliable. According to Norton, "You'd never leave your passport laying around your hotel room, giving access to your personal identity. But by using unsecured public Wi-Fi while you travel, you could be exposing data that could make your online accounts vulnerable and put you at risk for identity theft.."

8. Is my network in my office safe? Do I need an IT company to help set it up?

Depending on your level of security, your business network may not be safe. To increase your safety, be sure to have separate wifi access for guests, change the default password for the router, use a VPN, use WPA2 encryption, and stay up to date with software updates.

9. Does my email extort data from my conversations?

Using certain email providers, like Gmail's free accounts, opens your emails up for data extortion. This is ultimately a huge red flag for data security. The Verge says, "Gmail's access settings allows data companies and app developers to see people's emails and view private details, including recipient addresses, time stamps, and entire messages. And while those apps do need to receive user consent, the consent form isn't exactly clear that it would allow humans — and not just computers — to read your emails."

10. Can't I just train one of my employees to handle my IT needs?

Let's face it, Information Technology is evolving constantly. Training and equipping a staff member to handle your IT needs will, in the end, cost you more, and leave you open to possible threats that they just aren't prepared to handle. Client Tech specializes in conforming to fit the needs of a business' IT needs, rather than making a business fit their mold. Client Tech uses its knowledge to eliminate hackers and threats while increasing company security and digital protection.