



INSIDE THIS ISSUE:

5 Tips to Help you Take Control of Your Online Accounts **1-2**

PROS and CONS of BYOD **2-3**



- Abingdon Virginia, East
276-628-3838
- Abingdon Virginia, West
276-628-9558
- Bridgewater Virginia
540-828-2020
- Bristol Virginia, East
276-466-9222
- Bristol Virginia, West
276-669-1122
- Bristol Tennessee, Volunteer Pkwy
423-652-2022
- Christiansburg Virginia
540-260-9060
- Fairlawn Virginia
540-633-3793
- Gray Tennessee
423-467-9966
- Harrisonburg Virginia
540-434-0671
- Johnson City Tennessee
423-975-9900
- Kingsport Tennessee
423-246-3700
- Lebanon Virginia, East
276-889-3401
- Lebanon Virginia, West
276-889-4622
- Lynchburg Virginia
434-455-0888
- Norton Virginia
276-679-7401
- Staunton Virginia
540-885-8000
- Verona Virginia
540-248-7700
- Waynesboro Virginia
540-943-5020
- Wise Virginia
276-328-3439
- Wytheville Virginia
276-228-1125

5 TIPS TO HELP YOU TAKE CONTROL OF YOUR ONLINE ACCOUNTS

Many times cyber security tips are geared towards big businesses and organizations, and rightfully so. However, consumers have a stake in this game as well and need to be just as protected as businesses and organizations. If a particular account got hacked, someone can now access your information, alter the data, make fraudulent charges, or even steal your identity. As consumers, we must take control of our digital foot print and our accounts and make sure our digital assets are protected. Here are five tips that can get you on your way.

1.

We all know that our digital footprint is nearly impossible to be erased, so if you can't get rid of it, the next best thing is to try to make it safer. First things first: make a list. List all the sites that store your personal information, such as credit card information, pictures and videos and other important files.

2.

Put the most important accounts at the top of your list. Now that you have taken inventory of where your information is on the Web, the next step is to prioritize the most sensitive accounts and elevate your security levels to the highest available.

3.

Set the strongest possible access controls. Go through each important account, and one by one, set extremely hard passwords, change your security questions, and set higher levels of authentication and higher privacy settings where available. You'll also want to change your passwords more frequently for these accounts. And remember, your security questions don't have to be accurate; they just have to be memorable and difficult for a hacker to guess.



4.

Make sure you install your patches. Keeping up to date with security patches is a must. Your operating system, browser, and anti-virus applications all should have the latest security patches to protect against viruses and malware.



5.

Last but certainly not least: have a backup plan. All businesses have (or should have) a business continuity/disaster recovery (BC/DR) plan and consumers should as well. Your personal BC/DR plan should consist of a way to help you continue your “operations” in the event any of your accounts are compromised. Be sure to have a list of your account numbers and related contact phone numbers readily available.

Many attacks are successful because so many times, we fail to apply simple security safeguards. If we implement the above five steps, we can add an extra layer of protection that can go a long way in making it harder for us to become victims.

Sources:
<https://medium.com/future-crunch/9-easy-steps-to-take-back-control-of-your-digital-life-681a3899ab2f>
<https://www.realsimple.com/work-life/technology/safety-family/take-control-of-your-online-identity>
<https://theitguide.gizmodo.com/18-ways-to-make-your-online-accounts-more-secure-1793250264>

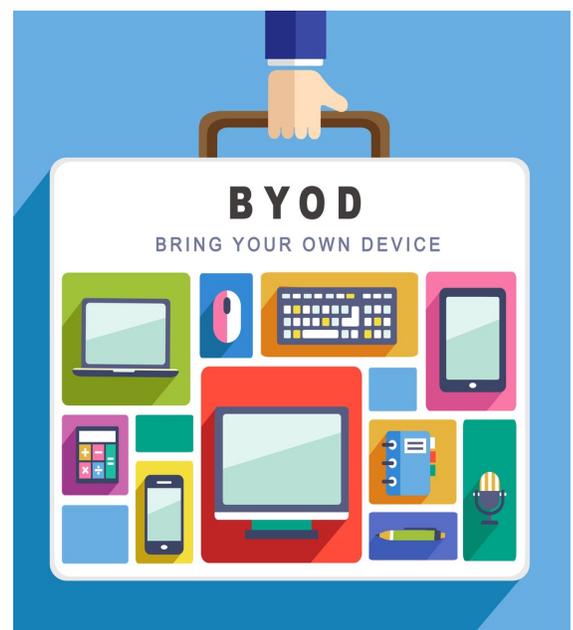
PROS AND CONS OF BYOD

Bring Your Own Device (BYOD) refers to the policy of not only permitting employees to bring personally owned devices (laptops, tablets, and smart phones) to the workplace, but also allowing the use of those devices to access privileged company information and applications.

BYOD has spiked in popularity over the past several years. It has some great benefits; however, there are some risk factors as well. Below are both some of the pros and cons of BYOD that everyone should consider.

PROS

- ⇒ Your employees are happy. No company can survive without hard-working employees. BYOD has allowed employees to use devices that they like and are familiar with to get their daily duties accomplished, allowing them to be more productive. It eliminates training time, and in turn saves the company money.
- ⇒ Reduces cost. The cost of purchasing devices for all employees can be reduced significantly by allowing employees to use their own devices. Studies have even shown subsidizing employees data plans cost significantly lower than buying the devices.
- ⇒ Flexibility. Having an employee use their own device rather than an in-house workstation allows them the flexibility to perform their job duties anywhere in the world. Samsung did a study that showed 78% of workers who used a single mobile device for work duties increased productivity.



Continue page 3

CONS

- ⇒ Security. This is the biggest concern for every company. A device used for company and personal use would still need to make sure it follows the company's security guidelines, such as appropriate antivirus protection, backup software, restricting Wi-Fi use and password protection.
- ⇒ Devices may not always be compatible. Not all the devices will be unified which may cause a problem when accessing certain applications.
- ⇒ Privacy. Privacy can be a major concern for both employee and company. When an employee uses their own device, they still have to follow the company security guidelines which will grant them access to the device. That means the employee's personal information that is on the device is accessible as well. For the company, the employee will have access to sensitive material that has the potential of being exposed if an employee leaves the organization. This leaves a company open to data leaks, whether intentionally or unintentionally.



BYOD is becoming more common; however, there is a lot to consider before implementing. It is important to know the pros and cons of this new trend and how it can impact your business.

Sources:
https://en.wikipedia.org/wiki/Bring_your_own_device
<https://www.techradar.com/news/computing/what-is-byod-and-why-is-it-important-1175088>
<https://www.thebalancecareers.com/bring-your-own-device-byod-job-policy-4139870>