info@comarcyber.com
comarcyber.com

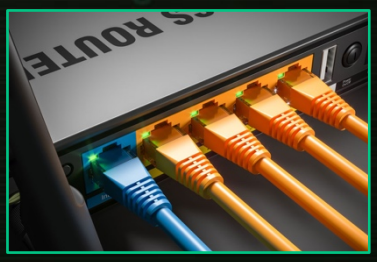
Work from Home Cyber Security Recommendations

Backup Before You Start!

Use 3, 2, 1 backup system: keep 3 copies of your data, 2 on physical media and 1 in the cloud. Use two different types of media, a portable hard drive and a thumb drive for example. Use an online backup service with automatic, scheduled backup sessions like Carbonite.com.

- Arrange backup system NOW! Before you start or continue working.
- Back ups should be in **THREE (3)** different places in **addition** to your computer:
    - Cloud backup: many services – Google Drive, Dropbox, Box.com. You can keep it simple and free with Google Drive or OneDrive or more complex if you need to network with many people on the same cloud.
    - Physical hard drive you keep in your office/workspace.
    - Keep one physical backup off-premises if possible, or on a thumb drive.

Switch to a Better Router



Modern mesh routers are better than the one bundled with the cable company's offerings. While they don't have built in security software, they add to your home network's security because they all have smartphone apps that allow you to see at a glance what devices are on your network, and to limit their access if you choose. These multimode systems also allow for greater coverage in larger homes. The best are: Eero, Orbi, and Velop.

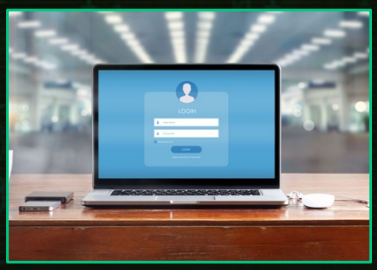
Use a VPN for Sensitive Work

Depending on the level of sensitivity of your work, consider using a VPN at home. DEFINITELY use one when working over wireless internet connections outside of your house. Never use a free VPN. They sell data about what sites you're visiting and your location to make money. Avoid paid or free services based in China or other countries with questionable corporate privacy laws & practices. Best paid services include: NordVPN, ExpressVPN are leaders.

Consider Using a VPN installed in a Router

Sabai Technology sells routers with VPN pre-installed. This lets every device that connects to your Wi-Fi connect to a VPN automatically.

info@comarcyber.com
comarcyber.com



Create a Regular User Account

If you're using Microsoft Windows for your operating system and you only have one account on your machine, you're doing it wrong. Add another account and make sure it is a Standard User rather than an Admin User. Admin user accounts can add software and make changes to the operating system without a password. You have to have an admin account, but you don't need to do your daily work in it. When you do want to add new software, you can click on the option to "Run as Administrator" for that one instance of installing the software.

Use Computer Security Software

Use anti-virus. Some of the best are Bitdefender, Norton, MacAfee etc. Kaspersky is highly rated, but the US Government has stopped all use of their products due to possible ties to the Russian government, so be advised. Whichever software you use, start at the highest levels of security they offer then reduce protection as you need if you find yourself getting too many false alarms.

Malware Detection

In addition to antivirus also use Malware Bytes or equivalent. This is real time protection that will often block threats as soon as they are clicked on.

Use Password Manager Software

You need a new, random password for every website you create a login for. People aren't good at generating new passwords (they typically rotate parts of passwords they've already used), random passwords (funny story about most people's idea of random), and no on can remember the average 23 passwords most people have for all their online services. Password managers securely keep and generate strong random unique passwords. They can also automatically insert the passwords into login pages as soon as you get to an account you have a password for. Some questions the security of all your password eggs in one basket approach, but it's been proven to be more secure than you using Password123! and 123Password! over and over. Highest rated password managers are: LastPass, 1Password, Bitwarden, Dashlane, and Keeper.

info@comarcyber.com
comarcyber.com

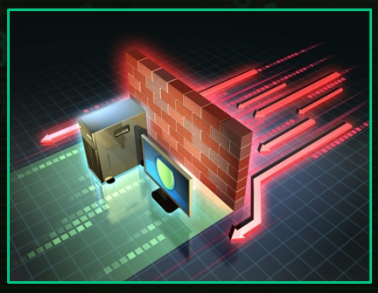
Encrypt Files at Rest

Use full disk encryption when possible. In addition, consider programs that allow you to encrypt individual files or folders. You can also encrypt individual files and email them or share them on a thumb drive securely. TrueCrypt is a good option.

Use Two-Factor Authentication

Software or devices that generate a verification code number you use in addition to a password. Google HQS began using YubiKey and their email takeover rate went to zero. Use either a software version on smartphone or a hardware token or key:

- Authenticator apps from Microsoft or LastPass
- Hardware – tokens that generate authentication numbers or plug in devices like YubiKey



Consider a Hardware Firewall to Prevent Internet of Things (IoT) Attacks

Hardware firewalls help screen malware at the Wi-Fi router. Malware that comes in from the Internet will be screened out. Devices with malware that connect to your router such as guest laptops & phones will also have their malware screened out too. Box by Bitdefender and Norton's Core are top products.