Edafio TECHNOLOGY PARTNERS

7 TIPS TO IMPROVE CYBERSECURITY FOR YOUR HOME (AND A COUPLE BONUS TIPS)

YOUR GUIDE TO PROTECTING YOURSELF AND YOUR BUSINESS WHILE YOU WORK FROM HOME.

As more of us are working from home, cybercriminals are using this transition to find security lapses to exploit while we are more vulnerable. What other steps can you take to secure your home network beyond your organization's cybersecurity policies and practices?

These are a few security measures that you can take to minimize the risk and protect not only your organization but yourself and your family's information while you work from home.

CHANGE DEFAULT PASSWORDS

Devices provided by your Internet Service Provider (such as a modem or wireless router) or purchased independently often come with default passwords to access the Administrative side of the device. These passwords should be changed immediately as they are often easily compromised by bad actors.

SOME BEST PRACTICE TIPS FOR CREATING A STRONG PASSWORD INCLUDE THE FOLLOWING:

Using a passphrase that is easy to remember but complicated to guess.

For example, G!ueC@rM0dleH0bb1e or I love NFL football!

A password should be at least 12 characters with capital and lowercase letters, symbols, and numbers.

Never use the same password across multiple accounts.

Instead create unique passwords for every account using a password manager.

Password managers can generate, autofill and store passwords securely. Some also allow for family sharing.

Typically, the device will list a default IP address and Admin password either in its documentation or on the device itself.

Below are links to some of the ISP Help pages on how to change the default password:

AT&T

Comcast

Cox Communications

Windstream

SOFTWARE IS UP TO DATE

Check that all security software is up to date: Privacy tools, add-ons for browsers and other patches need to be checked regularly on all your home devices (tablets, laptops, phones, etc.). Ensure Operating System (Windows, MAC) updates are up to date (**DO NOT** allow Windows XP or Windows 7 to connect). Review unused software that is installed on the device by default (Examples include Games, anti-virus trials, office trials) and uninstall.

ENABLE MULTI-FACTOR OR TWO-FACTOR AUTHENTICATION

Where possible, enable multi-factor or two-factor authentication (MFA or 2FA) as an additional layer of security. Here are some links on how to enable MFA for common social network sites.

LinkedIn
Twitter
Facebook
Instagram
Snapchat
TikTok
Steam

ANTI-VIRUS

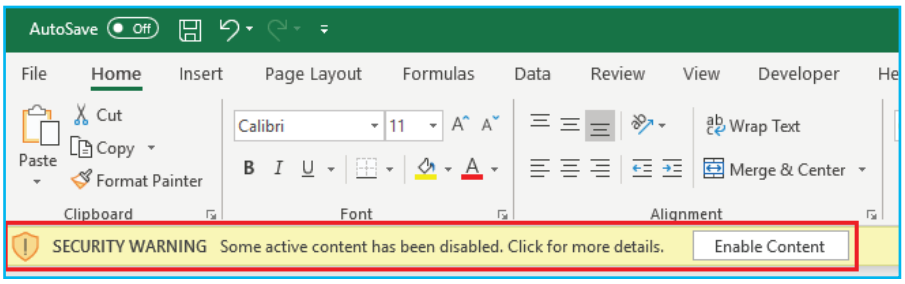
ENSURE ANTI-VIRUS IS IN PLACE AND FULLY UPDATED ON YOUR DEVICES

A system without an antivirus is just like a house with an open door. An open and unprotected door will attract all the intruders and burglars into your home. Similarly, an unprotected computer will end up inviting all the viruses to the system. Antivirus software will act as a closed door with a security guard for your computer fending off malicious viruses.

Here are a couple examples.

Name	Free Version	Paid Version	Notes
Bitdefender	Yes	Yes	Free version has the same core Anti-Virus protection as the paid version. Free Version offers Web Protection. MANY Additional/Enhanced features in Paid Version. Free version does NOT support MAC devices. Free Version does not include Parental Controls.
Sophos Home	Yes	Yes	Free version has excellent scores in independent testing. Free version has web filtering and browser features. Free Version includes Parental Controls. Free version limited to 3 devices.
Microsoft Windows Defender Security Center	Yes	No	Built into Windows 10. Good lab scores. Limited to Windows. Web protection only works on Microsoft Browsers. Awkward Scan Scheduling.

DISABLE MACROS IN MICROSOFT OFFICE PROGRAMS



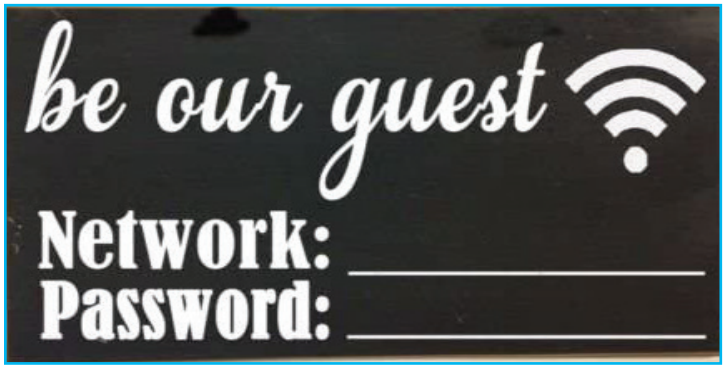
The 2019 Verizon Data Breach Investigations Report found that 90% of emailed malware is distributed via macros. For end-users, we always recommend that you don't enable macros on documents you receive from a source you do not trust or know and be careful even with macros in attachments from people you do trust – in case they've been hacked. To take it a step further, unless there's a viable need we recommend changing your settings on any personal devices that use Microsoft Office programs to disable all macros without notifications.

IMPORTANT: WHEN YOU CHANGE YOUR MACRO SETTINGS IN THE TRUST CENTER, THE MACRO SETTINGS ARE NOT CHANGED FOR ALL YOUR OFFICE PROGRAMS.

HOW TO DISABLE:
For **each** Microsoft Office Program (examples include Word, Excel, PowerPoint)
Open the Document > File tab > Options > Trust Center > Trust Center Settings > Macro Settings > Disable all macros without notification.

CONSIDER SETTING UP A HOME GUEST NETWORK

We've all had friends or family come to visit and we've handed out our wireless password for them to access without thinking twice about what they download or what they already have on their devices and how that could spread to your own devices.
Additionally, your "Internet of Things" (IOT) devices at home can – and as some sources have stated – will at some point be hacked.



The way to isolate and lower the risk of malicious programs/activities spreading from your guest's devices or IOTs to your computers, tablets or printers is to keep those devices segmented from your network via a guest network.

Recommend implementing a guest network for guest access, and then optionally research how and what to migrate (IOTs) to a guest network.
Here are a few Internet Provider (ISP) resources about setting up home guest networks.
Contact your ISP for more information on how to set up a guest wireless network.

AT&T

Cox Communications

SECURE YOUR IOT DEVICES (INTERNET OF THINGS)

IOTs in our home include Smart devices, such as a TV or thermostat, as well as that baby camera, front door security camera or even game consoles.

These devices require special consideration because they can be particularly vulnerable to attackers. Besides segmenting these devices to a guest network here are some additional tips to keep your IoT devices more secure.

• Change all default passwords and, if possible, enable multi-factor authentication (MFA) on accounts linked to devices.
•Update firmware and software for the devices regularly.
• Disable unused features such as Bluetooth.

ADDITIONAL RECOMMENDATIONS

• Use a company-issued VPN to access work accounts.

• Consider turning off digital personal assistants (such as Alexa and Siri) while you are workin from home in order to protect the confidentiality of your organization's information.

• Be aware of family or friend's exposure to work calls and video conferences and limit as much as possible in order to respect confidentiality.

• Do not download programs, files, or add-ons unless they come from legitimate, verified sources.

• Any email or site discussing COVID-19 should be suspect. Attackers are using the pandemic to phish people in order to install ransomware or compromise accounts.

• If you're connecting your work computer to your home network, make it not visible to other computers in the network and the option to share files is off.

• Don't recommend sending work emails on your personal email account.

• Keep personal use, such as children's schoolwork, separate from your work device.

RESOURCES

https://www.knowbe4.com/coronavirus-security-awareness-resources
https://staysafeonline.org/covid-19-security-resource-library

IT CONSULTING & MANAGEMENT | CYBERSECURITY | CLOUD-COMPUTING | HEALTHCARE CONSULTING

WHAT'S NEXT?

Get started on your IT transformation today. Learn about how our customizable consulting services can help your business stay on track.

OTHER CYBERSECURITY SERVICES:

Best in class cybersecurity depends on multiple layers, and below are some of the cybersecurity offerings we provide our clients:

- **Security Risk Assessment**
- **Compliance Consulting**
- **vCISO (Virtual Chief Information Security Officer)**
- **Continuous Vulnerability Identification**
- **Information Security Program Management**
- **Cybersecurity Policy and Procedures**
- **Incident Response**
- **E-mail Encryption Services**
- **Internet/E-mail filtering, monitoring and reporting**
- **Centralized Anti-Virus Solutions**

ABOUT EDAFIO

We take the time to get to know your business inside and out to better serve you. By investing in relationships with our clients, we're able to meet challenges as they arise and offer the best custom solutions as technology changes.

Edafio has been successfully assisting medium to enterprise-sized organizations in selecting, implementing, and optimizing IT consulting and management, cybersecurity, healthcare consulting, and cloud computing solutions across multiple industries from our offices in Central and Northwest Arkansas.