Relativity®

Maximize Cybersecurity at Home

10 Ways You Can Go Above and Beyond to Protect Your Data while Working Remotely

The COVID-19 crisis is having an unprecedented effect on the day-to-day operations of companies around the globe. With stay-at-home orders and quarantines in place, collocated offices are shutting down and home offices are getting more use than ever.

For many in the legal field, work isn't stopping—and moving it can be a source of discomfort. Accessing sensitive company and client data from an IT-protected, secure network is one thing; accessing it from your kitchen is quite another. But there are ways to ensure you're keeping that data secure, and in many cases, you can implement them on your own.

Take a look at these 10 focus areas to ensure you're keeping sensitive information as safe as possible.

01

Device Inventory

What should you do?

Document which devices you use to access your network and any business data.

Why and how should you do it?

When chain of custody, discoverability, and security are called into question, understanding how and by whom data is accessed is key. At the office, your IT team keeps track of the devices employees are using on the company network and understands how they're accessing important data.

At home, the best way to know what is on your network—and be prepared to let your team know, should it become necessary—is to take an initial inventory of all the devices you plan to put on the network. This can be as simple as taking a picture and grabbing the MAC address from each device (including laptops, tablets, and smartphones) for later reference.

You can also find an inventory of devices connected to your network via your access point or router. That's a simple way to determine who is connected by hostname, MAC address, and IP address. See your device manual for more information.

02

Device Security

What should you do?

Follow basic best practices for device security while you’re working remotely.

Why and how should you do it?

At home, where you’re used to browsing social media, streaming movies, and sharing photos with friends and family, it can be easy to forget basic security protocols that come naturally at the office. Don’t let that happen.

For instance, make sure you are still following best practices for password hygiene. These include:

- Don’t reuse passwords on your devices.
- If you can use a password manager, do so. It will allow you to create more complex passwords.
- If biometrics are an option on your devices, use them. It’s harder to spoof a fingerprint than to see what you are typing as you enter your password to check your email while you’re at the grocery store.

Additionally, ensure that every device on your network has endpoint antivirus protection. This will stop known malware from executing on your devices—or at least make it more difficult to do so—and give you alerts so that you are aware of dangerous activity. Run regular scans and keep this protection up to date.

Remember that any device connected to the internet is susceptible to viruses, malware, and attacks. Don’t make it easy for bad actors.

03

Firewall / Router Configuration

What should you do?

Set up your home network defensively.

Why and how should you do it?

Your router—and the firewall it establishes—is crucial to securing your network. This device is most secure when its management page or interface is not open to the public internet. If your device has the option to be managed from the internet, make sure that option is disabled. Enabling it allows unauthorized actors to attempt to log in.

It should also be obvious that having a simple or default password for accessing your router is the worst thing you can do. Make this device's password as complex as possible, but easy for you to remember—or use a password manager to remember something more complex for you.

04

Port Forwarding

What should you do?

Limit port forwarding as much as possible.

Why and how should you do it?

Forwarding a port is a way to access a device from the internet even when you aren't physically using that device. Using port forwarding, you are hosting a private server on your local network that is accessible from the internet. For example, websites are accessible via open ports on web servers.

If a port does not need to be open, don't have it open. Having too many open ports creates a window for intrusion. At home, port forwarding may be required for gaming and other use cases. If you need to access a machine remotely, consider having a VPN server set up within your network and only leave that required port forwarded. In doing so, you will have access to your devices throughout your home network and limit the attack surface.

Learn more about port forwarding at home at this website:
https://stevessmarthomeguide.com/understanding-port-forwarding

05

VPN Management

What should you do?

Consider using a personal VPN within your network.

Why and how should you do it?

If your router or firewall can run a VPN server, consider setting it up. It will enable remote access to your devices while limiting who else has access to them. VPNs are especially beneficial if you're using a shared WiFi network, such as a free access point set up by your internet provider or a shared WiFi hotspot.

If your router or firewall cannot run a VPN server, a similar workflow can be accomplished with alternatives such as a Raspberry Pi, a Virtual Machine, or even an unused computer. OpenVPN is the most common opensource VPN protocol.

Visit this page to learn more about whether a VPN is right for your circumstances:
https://www.pcmag.com/news/do-i-need-a-vpn-at-home

06

VLAN Setup

What should you do?

Use a VLAN to prevent cross-contamination of data.

Why and how should you do it?

A simple way to prevent your devices from talking to other devices they shouldn't is by creating a Virtual Local Area Network, or VLAN. This creates a separate network on top of your current network by "tagging" traffic as you specify.

This is a useful strategy for separating your business devices from personal and even Internet of Things (IoT) devices, such as a smart refrigerator. A VLAN creates another layer of security in that IoT devices won't be able to talk to your business devices unless you allow them to.

For detailed instructions, see these resources:

- **https://computer.howstuffworks.com/lan-switch16.htm**
- **https://www.inteltech.com/blog/how-do-vlans-work**

07

IP Assignments

What should you do?

Have IPs assigned appropriately for different devices and networks.

Why and how should you do it?

Separating IPs will designate which devices access what via the internet and minimize exposure of sensitive information. If you created a VLAN, you will need to assign IPs to the devices that will occupy that IP subnet. You will also need to specify the IP range in your DCHP settings to ensure devices joining that subnet are automatically assigned an address without opening too many doors to unauthorized use. Knowing how many devices you plan to put on each subnet will help you choose these settings appropriately.

Visit this link for an easy table outlining your options for IP ranges:
https://dnsmadeeasy.com/support/subnet

For example, say you have 10 IoT devices in the IoT VLAN you've created. You should use a /28 subnet, because that gives 14 useable addresses for individual devices, offering a small window for expansion—as opposed to a /24, which will give you a window of 254 useable addresses (a bit too much for a subnet that will host your most vulnerable devices). On the other hand, when it comes to having a locked-down subnet for business use, a /29 should do fine as it will give you space for 6 devices.

08

DNS Security

What should you do?

Ensure your DNS is using a trusted service IP.

Why and how should you do it?

A Domain Name Service or DNS is the way that a device exchanges a request for a website. The website DNS will return its IP address based on records that the root DNS servers send back. This can be one way to show network traffic, as these requests are visible if someone examines the request—including a threat actor.

With this information, a malicious actor can see where you are trying to go and possibly redirect you to a spoofed website. It is important to know what your DNS server IP is, and make sure that your router is pointing to a known and trusted DNS service IP (1.1.1.1 or 8.8.8.8 are two examples). This precaution will ensure that your server always points your requests to a root DNS server and prevents your traffic from getting redirected.

Learn more here:
https://www.cloudflare.com/learning/dns/what-is-dns

09

SSID Settings

What should you do?

Be smart about the name and protection you give to your wireless network.

Why and how should you do it?

Your SSID is the name that you—and others—will see when attempting to connect to your wireless network.

Don’t make it obvious with regards to whom the network belongs to (i.e., “Smith’s WiFi”). Instead, make it something unique that you can easily recognize, but unintuitive enough for someone on the outside not to know whose network it is. Doing so makes it harder for someone sitting outside to break into your network wirelessly.

If you decided to set up a VLAN for your IoT or business devices, you will need to set up separate SSIDs for each network.

Make sure that each SSID has a strong password that is not easily guessed, and never use the default password that comes with your access point or wireless router.

Also, be sure to never leave a WiFi network unencrypted. Set an encryption protocol such as WPA2-PSK so your traffic is encrypted from your device to the access point. Never use WEP as a form of encryption, as that protocol can be compromised in a matter of minutes.

10

Basic Precautions

What should you do?

Beware of your internet use and keep devices updated for better ongoing cybersecurity.

Why and how should you do it?

Important as these advanced measures may be, you'll still need to practice ongoing security mindfulness. Basic precautions for everyday internet browsing should be followed on the devices you use to access data for work, as well as other devices on your home network. These precautions include:

- Make sure every website you use is "HTTPS" and that it has a valid certificate.
- Only visit URLs you trust or have visited before.
- Never click on unknown or suspicious links. Watch for doppelganger domains.
- If you have to log into a page, don't get there by clicking on a link—especially one from an email. Instead, use bookmarked pages or manually type in the URL.

And finally, the most important thing to do to prevent your network from being compromised is keeping all of your devices up to date. An out-of-date device leaves room for exploitation and can be either used for traversing through the network or as part of a botnet. If your device no longer receives software or operating system updates, it should not be connected to the internet. Instead, put it behind the firewall and only allow it to be accessed from the VPN or from within the same network.

Relativity®