Work From Home Security Guide

In Plain English...

Like many others, you may have been caught off guard by the Coronavirus and your entire team is now required to work from home. I posted the following question on LinkedIn, “What can companies do to address the risk of people using their personal computers and home networks to access sensitive data?”. And many of you responded; your suggestions were a treasure trove!

This quick guide is based on your responses!

Gabriel Friedlander
https://www.linkedin.com/in/gabrielfriedlander/

Security Mindset

Before we begin, there are a few common beliefs that have to do more with mindset than technology.

Get Up, It's Time to Go to Work

You are at home but you are actually at work, so don't work from bed… find a place and make it your office. Let your family know that this is your office and it's not to be shared with others while you are working. And remember, Starbucks is not your home…
home is where you wake up every morning and not a public place. Make sure confidential information is not laying around and lock your computer when you are not next to it. Don't email documents to your home printer or to your personal email just to make it easy
to print.

Smile, You Are on Camera

Communication and collaboration is another big topic and technology will play a major role. You will probably need to over communicate using tools like Teams, Slack, or Zoom (so get out of your PJs…) and don't use WhatsApp, Facebook, LinkedIn, or any other personal or social app to communicate. Only use the tools approved by your organization and apply even stricter security measures than for email (for example, don't share passwords on Slack).

Polices, Procedures, and Awareness

Before we talk about technology, it's important employees understand what is expected from them. Work with your HR/Training department on putting together a mini orientation on remote work.

Update Your Security Policies

Time to refresh your BYOD and Remote Work policies. If you don't have anything… create a list of the most critical Security Policies/Rules and share it with all remote users. This is a great reason to revise your existing security policies and train your team.

Security Awareness Starts at Home

Your manager is not sitting next to you anymore, so it's important now more than ever to refresh your security awareness training and reinforce some of the basic security rules, such as call over the phone and verify any request to share confidential data or transfer funds. In addition to standard training, also provide home security awareness, e.g. don't have work sensitive conversations near IOT devices like Siri, Alexa, or Google Home in case they're listening. Devices are not to be shared with other family members and they must have a unique password and a lock screen timeout.
There are some great paid and free security awareness solutions that include both business and home user training such as https://wizer-training.com (this is our solution...).

Now, Let's Talk Technology

Because this is a quick guide, I focused on the "quick wins" that organizations can achieve in a short amount of time with an affordable budget. Obviously there is much more that can be done depending on the budget and maturity of the organization (Monitoring, Logging, Network Segregation, Identity Management etc...), but I think this is a good starting point.

Provide an Isolated Environment to Work From

Since you're most likely unable to control remote worker devices, you'll want to isolate work related activities from the home network as much as possible. If available, provide employees with company laptops that are hardened (VPN, endpoint security,
patched, and the items listed below). These devices should be used strictly for organizational work only. If this is cost prohibitive or too time consuming, then provide them with pre-configured Virtual Desktops. You can either have these virtual desktops run on their personal computers (assuming their hardware supports it…) or consider azure-based virtual desktops users can remotely connect to. In any case, avoid a solution where employees share a computer for both work and personal usage, and only use the Admin account when authorized and not for routine work.

Support Hotline

Non-technical people should not perform technical tasks; this could lead to even greater risk. So set up a hotline and make sure users know who to contact in the event of technical issues. Maybe it's time to upgrade the ticketing system…

VPN

Set up a company VPN and require it to access the office network and resources. And make sure the firewall and infrastructure can handle all the "new" inbound traffic.

MFA

Many times MFA is enabled but not enforced, so make sure it is enforced for all users and apps. If hardware tokens are too expensive, use an Authentication App on a smartphone rather than 2FA (Text messages).

WiFi

Many times MFA is enabled but not enforced, so make sure it is enforced for all users and apps. If hardware tokens are too expensive, use an Authentication App on a smartphone rather than 2FA (Text messages).

Complex Passwords

Users should avoid saving passwords to their browsers. They should use long and complex pass-phases and never reuse them. Also, use unique passwords for Wifi, Apps, Router, etc...

Safe Browser

It’s advised to use a secure browser like Brave Browser, which is also faster.

Keep Your Device Updated

Apply the latest security patches (OS and Apps) and avoid outdated operating systems like Windows 7 or XP across both virtual desktops and personal

computers. Keep only apps that were approved by the organization (uninstall all others) and turn on Automatic updates.

Endpoint Protection

Use a NextGen anti-virus solution on all remote devices.

Firewall

Make sure the built-in firewall is properly configured and always enabled on remote devices.

Backup

Users should know how and where to backup their data, don't rely on them to come up with a solution. Preferably an encrypted offline backup.

Encryption

Encrypt files stored on devices. Many options exist for protecting files including encrypting individual files or folders, volumes, and hard drives, and avoid using removable devices such as USB sticks.

Additional Useful Resources

From National Institute of Standards and Technology (NIST): User's Guide to Telework and Bring Your Own Device (BYOD) Security
https://www.nist.gov/publications/users-guide-telework-and-bring-your-own-device-byod-security

From Center for Internet Security: CIS Controls Telework and Small Office Network Security Guide
https://www.cisecurity.org/white-papers/cis-controls-telework-and-small-office-network-security-guide/

On a personal note, I believe this huge increase in working from home will change the world as we know it. Organizations will realize working from home is not such a bad idea and could overall reduce operational costs. It will create an opportunity to hire skilled employees regardless of location and provide a better life/work balance. I think companies need to quickly adapt and use this as a catalyst to develop a secure environment for this new work from home culture.

Gabriel Friedlander,
Wizer's CEO