Privacy and Security Recommendations for OPI Remote Workers

In the office there are systems / controls / processes that protect our computers and networks. They include firewalls, automated patching and updates, ongoing monitoring, and many more. When working from home or remotely most of these protections are not available. In these situations, the state and OPI are relying on each of us to use our training and good judgement to protect OPI's resources, data and reputation.

What are the additional security risks of remote and at home work?

- **Increased risk of malware infection** – With fewer security controls protecting our systems, it is much easier for a system to become infected with a virus / malware.

- **Man in the Middle attack** – A hacker may attempt to insert themselves in the middle of your computer traffic where they can steel user names and passwords.

- **Sniffed Network Traffic** – Similar to the man-in-the-middle attack, a hacker may use hardware or software to listen to our computer traffic.

- **Hacked system through home network vulnerability** – Outdate or unpatched home network equipment provide opportunities for malware or hackers to access and infect our system.

What creates the additional risk with remote and at home work?

- **Outdated home network equipment** – If your home WiFi / ISP router equipment is more 3 or 4 years old it is likely no longer support by manufacture patches and updates. This creates vulnerabilities that can be exploited by malware or hackers.

- **Unpatched home network equipment** – nearly all computer systems and equipment need ongoing software patches and updates to be fully protected. This is often a manual process that should be completed on regular basis. To keep your home network protected you should know your WiFi / ISP router make and model. Browse to their site and find the instructions on how to complete updates on your equipment. Then complete the patch installation.

- **Security features not enabled on home network equipment** – Many of the newer WiFi / ISP routers include additional security features such as virus / malware scanning or malicious traffic blocking. These features may require some setup to be fully activate. Please find the brand and model of your equipment and contact the manufactures website to learn how to fully enable all security features.

- **Admin passwords not changed from defaults** – Most WiFi / ISP routers and equipment use generic administrator passwords for their equipment when they are shipped. These passwords are readily available on the Internet and can be used by hackers to gain admin access to your equipment. These passwords should always be changed to difficult passwords when you initially setup the equipment.

- **WiFi network names that disclose your identity (Address or your name)** – All WiFi networks require a broadcast name (SSID) that identifies them. It is recommended that you don't use your name of personally identifiable information when setting up our home equipment. This makes it easy to target your personal traffic if someone is so inclined.

- **Working on Shared / unsecured networks** – There are many different scenarios for connecting your system to the Internet. If you are considering remotely working from a restaurant / hotel / coffee shop… keep the following in mind:
  - Avoid using the public WiFi if possible and use your cell phone hotspot.
  - Wait and complete the work later from a known safe network.
  - If you must work from public WiFi try to avoid working with sensitive data / files
  - Use secure browser websites when possible: Https is your friend / Http is open and not secure.

- **Home network activity (logs and activity) not reviewed** – Most user are not experts on networking, but it is important to occasionally check for unusual activity… Has someone logged into your WiFi / ISP router in the middle of the night? Is there excessive network traffic during times when there shouldn't be? These are good things to check on.

Here are some recommendations for increasing your home network security:

- Replace outdated equipment
- Patch and update home network equipment regularly
- Change default passwords immediately
- Occasionally change WiFi passwords
- Change network broadcast name to something non-identifying if possible
- Monitor logs and activity of your home network