eSENTIRE

Working from Home

Securing your remote workers and home office

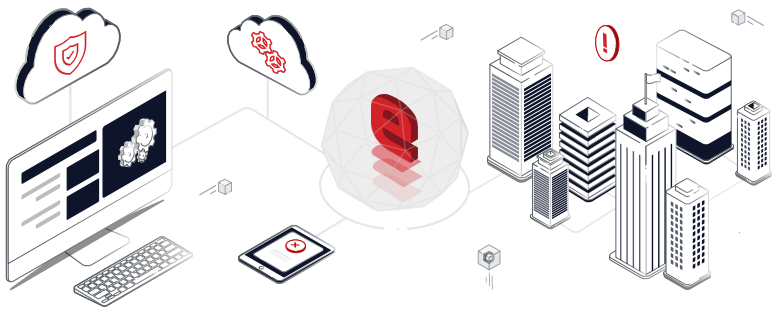
The current work-from-home climate that's become our new normal creates ripe opportunities for cybercriminals to exploit uncertainties created by companies scrambling to secure a remote workforce.

As workforces take shelter at home, the risk of attacks against corporate remote access systems goes up. Criminals are targeting employees to harvest their VPN credentials as a backstage pass to corporate assets. Here are a few actions you can take to protect your business and employees:

1. Revisit your business continuity plan (BCP)
2. Keep your employees informed
3. Use a VPN to protect and encrypt remote connections
4. Enforce multi-factor authentication
5. Disable administrative privileges
6. Protect your endpoints with detection and response
7. Manage BYOD devices with MDM/EDM services
8. Run a COVID-19 cross-function simulation

SEE EVERYTHING. MISS NOTHING.

Take control of your risk. Our cloud-delivered Managed Detection and Response (MDR) platform is purpose-built to find and stop threats in real-time across your digital landscape.



As we work from home we introduce new risk into our lives and businesses. Criminals are good at finding the weakest link and exploiting it. And workers, using consumer-grade internet connections at home, can quickly become that weak link. Here are tips to secure your home workplace:

Follow your company's policies: Most companies have deployed security measures to protect their employees. Always follow these procedures.

Keep informed about company updates: Obtain your information from your company and reputable news sources. Avoid social media for updates. These sites often contain false, misleading or malicious content and links.

Don't share COVID-19 information: Numerous scams and untested, unlicensed treatments have been reported. These sites can contain links to malicious websites, attachments that spread malware.

Keep your kids off your work devices: Many parents give their children access to their work computer or phone. Don't! Kids visit gaming sites and other social sites that often contain malvertizing or other suspect links.

Keep your devices up-to-date: These updates ensure your device has the strongest security profile. Devices with old software often fall victim to known and defensible attacks.

Conduct regular back-ups: Your company should have a back-up service configured on your computer. These services ensure you can quickly resume operations if a device is lost, stolen or disabled.

Securely dispose of sensitive data: Don't throw printed documents into your recycling. As we work from home, criminals know they will likely collect valuable information by grabbing a recycling box.

Use a password for online meetings: Always password protect meetings through online conference services. Criminals can scan for toll-free numbers or steal this information and eavesdrop.

Use strong passwords: Create a password of at least 12 characters composed of a mix of numbers, symbols and upper and lowercase letters. Avoid using replacement characters (zero for o, $ for s, ! for 1, etc.), repeating characters and incorporating personal identifiable information such as birth dates of loved ones or your home address. If you are concerned that your password is compromised, you can check it at **haveibeenpwned.com**.

Secure your home network: You are primarily secured by a consumer-grade router. There are 10 things you can do to reduce this risk:

1. Change the default SSID of your router
2. Enable WIFI encryption (WPA2 or WPA3)
3. Set a strong password for your WIFI
4. Change the default admin password
5. Keep your router's software up to date
6. Create a guest WIFI account and use a difference password than your WIFI
7. Position your router in the middle of the house to minimize the risk of outside connections
8. **Advanced:** Change the default IP address from 192.168.0.1
9. **Advanced:** Disable DHCP
10. **Advanced:** Disable remote access to the router

eSENTIRE