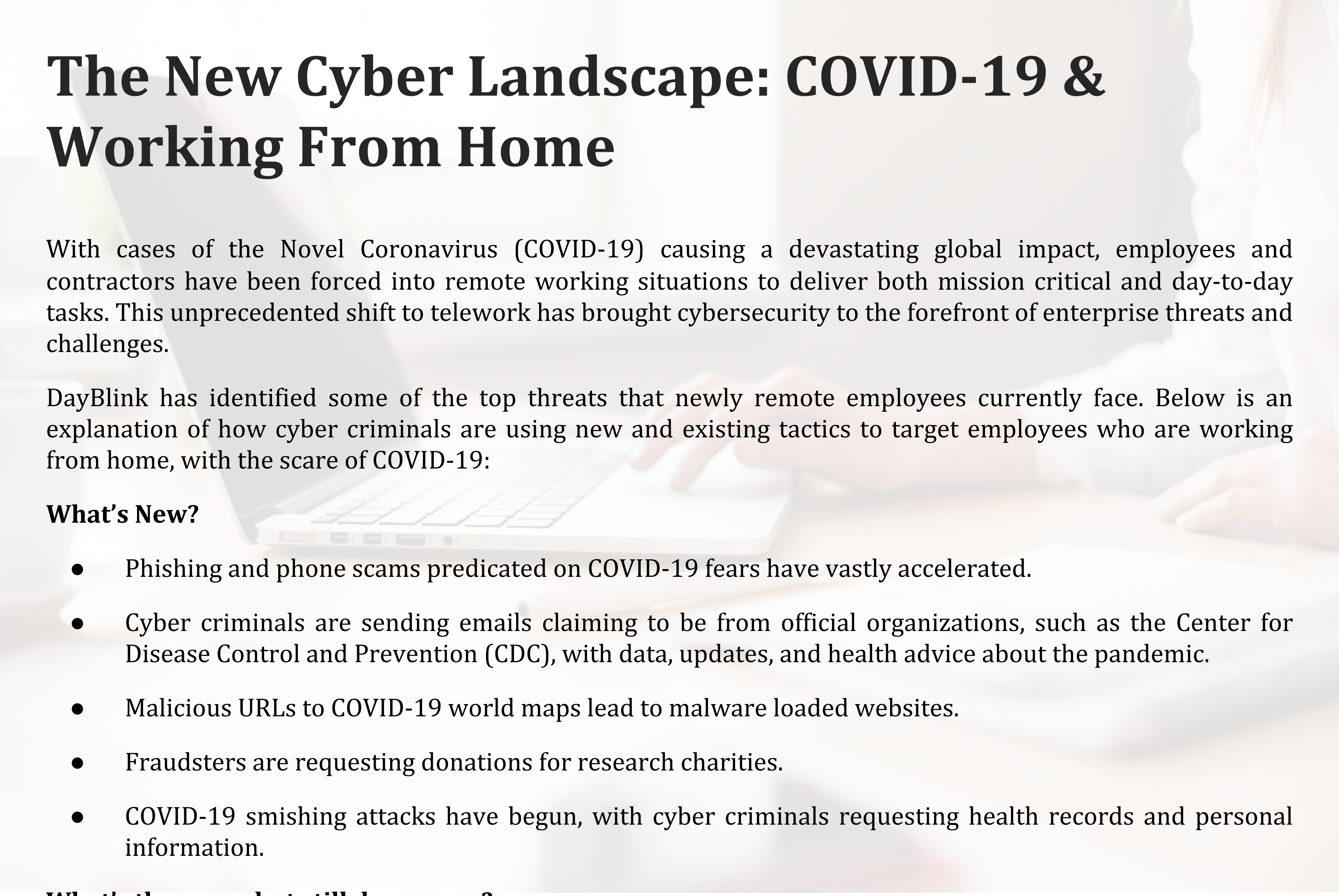


The New Cyber Landscape: COVID-19 & Working From Home

With cases of the Novel Coronavirus (COVID-19) causing a devastating global impact, employees and contractors have been forced into remote working situations to deliver both mission critical and day-to-day tasks. This unprecedented shift to telework has brought cybersecurity to the forefront of enterprise threats and challenges.

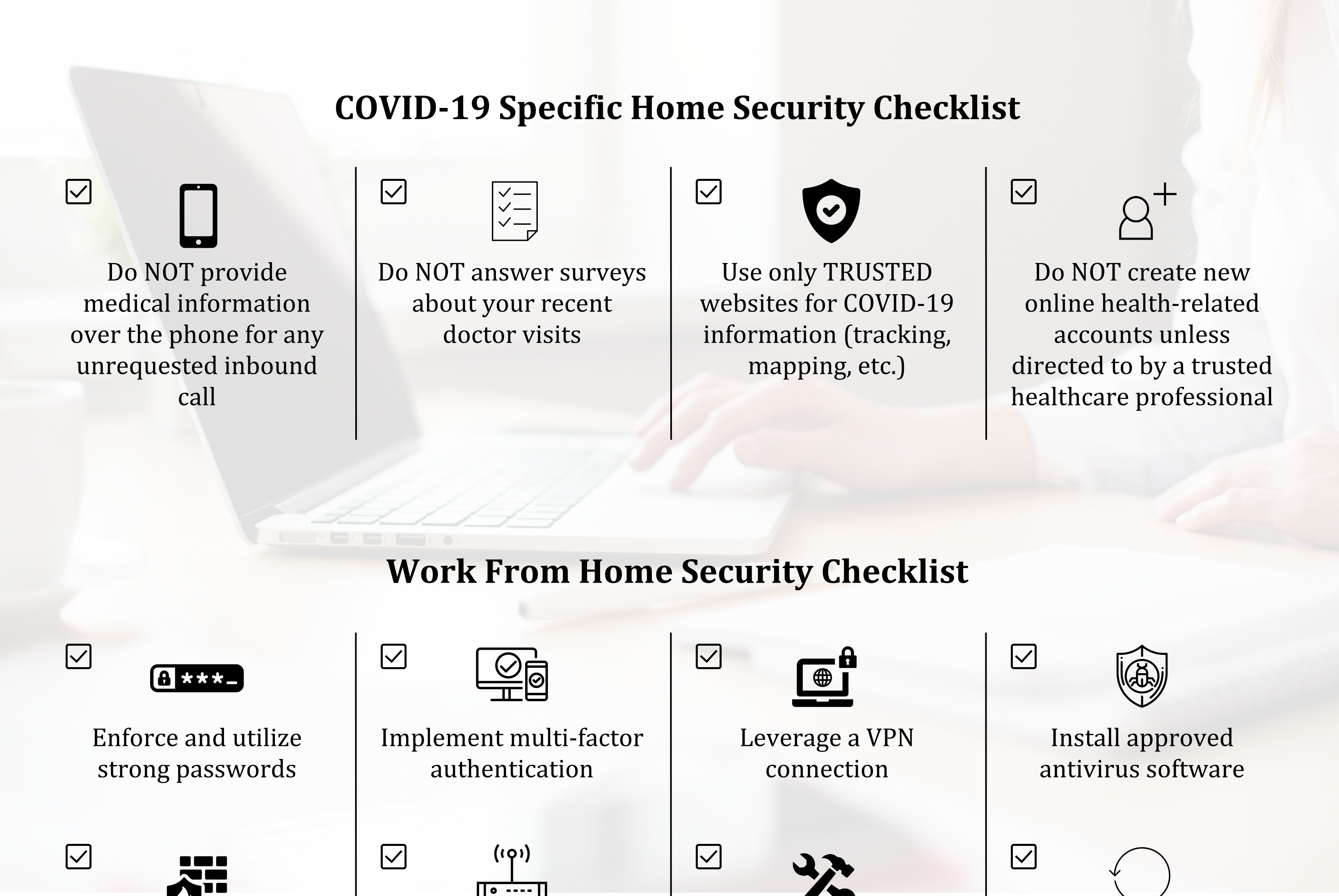
DayBlink has identified some of the top threats that newly remote employees currently face. Below is an explanation of how cyber criminals are using new and existing tactics to target employees who are working from home, with the scare of COVID-19:

What's New?

- Phishing and phone scams predicated on COVID-19 fears have vastly accelerated.
- Cyber criminals are sending emails claiming to be from official organizations, such as the Center for Disease Control and Prevention (CDC), with data, updates, and health advice about the pandemic.
- Malicious URLs to COVID-19 world maps lead to malware loaded websites.
- Fraudsters are requesting donations for research charities.
- COVID-19 smishing attacks have begun, with cyber criminals requesting health records and personal information.

What's the same, but still dangerous?

- Using a remote workstation without a VPN at home may leave your network exposed to hackers and ransomware attacks. Though painful, ensure you use separate credentials for your VPNs than for other logins (and while you are at it use LastPass or another Password manager to help you manage this).
- If not already enabled, Multi-Factor Authentication (MFA) is the easiest option to protect your VPNs from unauthorized access. This is a bonus as MFA will protect more than just your VPN (email, corporate applications, etc.).
- Whether or not you need a VPN, make sure to encrypt your local hard drives.
- Home and public WiFi networks along with hotspots are generally not as secure as a typical enterprise connection due to a combination of device vulnerabilities and weak password protection. Malicious cyber criminals may pose illegitimate WiFi networks as legitimate. This can lead to opportunities to monitor or log such connections in order to harvest confidential information. It's important to use secure connections only from trusted sources and avoid connecting with unknown wifi hotspots.
- Working from home increases the likelihood of data being compromised through external connected devices in a network (laptops, mobile devices, workstations, home smart devices, etc.).
- The strongest defense against this is to download an approved anti-virus software, use strong (long) password combinations, and connect to secure networks only.
- Remember to report any lost or stolen work devices immediately.



COVID-19 Specific Home Security Checklist

☑ Do NOT provide medical information over the phone for any unrequested inbound call

☑ Do NOT answer surveys about your recent doctor visits

☑ Use only TRUSTED websites for COVID-19 information (tracking, mapping, etc.)

☑ Do NOT create new online health-related accounts unless directed to by a trusted healthcare professional

Work From Home Security Checklist

☑ Enforce and utilize strong passwords

☑ Ensure firewalls are adequately set up

☑ Be aware of work from home scams

☑ Implement multi-factor authentication

☑ Secure home network and routers

☑ Safely store and lock up devices

☑ Leverage a VPN connection

☑ Beware of remote desktop tools

☑ Incorporate encrypted communications

☑ Install approved antivirus software

☑ Back up mission essential data

☑ Install latest software updates and security patches

It is important that everyone in your organization, especially those who work outside of the office, are up-to-date on all security procedures and policies. Businesses need to formulate recovery plans in case they are affected with a data breach or other incident as a result of work from home conditions. It is essential to maintain the bare backbones of infrastructure and functionality should an incident occur. DayBlink hopes that all employees ares well-informed, vigilant, continues to thrive, and successfully overcome all obstacles in today's complex and competitive environment with the COVID-19 pandemic.

If you have any questions regarding cyber threats related to COVID-19 or would like additional insight into implementing the cybersecurity measures mentioned above, please contact:
Michael Morgenstern (michael.morgenstern@dayblink.com), **Jacob Armijo** (jacob.armijo@dayblink.com),
Neeraj Dalvi (neeraj.dalvi@dayblink.com) at DayBlink Consulting.