Katten

CYBERSECURITY, PRIVACY AND DATA ADVISORY

Coronavirus Cyberhygiene: Dos and Don’ts for COVID-19 Remote Work

March 18, 2020

KEY POINTS

In the wake of the coronavirus (COVID-19) pandemic, government officials have urged companies to allow more employees to work from home in an effort to halt the spread of the disease. As businesses shuffle to operationalize remote work policies, bad actors continue to exploit the vulnerabilities associated with remote work and target employees working from home.

Below are a few tips to help employers address the security threats and challenges of remote work.[1] These include:

- Monitoring and awareness of cybersecurity threats as well as risk mitigation;
- Use of secure Wi-Fi networks, strong passwords, secure VPNs, network infrastructure devices and other remote working devices;
- Use of company-issued or approved laptops and sandboxed virtual systems instead of personal computers and accounts, as well as careful handling of sensitive and confidential materials; and
- Preparing to handle security incidents while remote.

Be on the lookout for phishing and other hacking attempts. Be on high alert for cybersecurity attacks, as cybercriminals are always searching for security vulnerabilities to exploit. A malicious hacker could target employees working remotely by creating a fake coronavirus notice, phony request for charitable contributions or even go so far as impersonating someone from the company’s Information Technology (IT) department. Employers should educate employees on the red flags of phishing emails and continuously remind employees to remain vigilant of potential scams, exercise caution when handling emails and report any suspicious communications.[2]

Maintain a secure Wi-Fi connection. Information transmitted over public and unsecured networks (such as a free café, store or building Wi-Fi) can be viewed or accessed by others. Employers should configure VPN for telework and enable multi-factor authentication for remote access. To increase security at home, employers should advise employees to take additional precautions, such as using secure Wi-Fi settings and changing default Wi-Fi passwords.

[1] For additional remote work recommendations from the Cybersecurity and Infrastructure Security Agency (CISA) “Alert (AA20-073A): Enterprise VPN Security,” Cybersecurity and Infrastructure Security Agency (CISA), March 13, 2020 (available at https://www.us-cert.gov/ncas/alerts/aa20-073a).

[2] For additional information from CISA regarding scams related to COVID-19, see “Defending Against COVID-19 Cyber Scams,” March 6, 2020 (available at https://www.us-cert.gov/ncas/current-activity/2020/03/06/defending-against-covid-19-cyber-scams).

Change and create strong passwords. Passwords that use pet or children names, birthdays or any other information that can be found on social media can be easily guessed by hackers. Employers should require account and device passwords to be sufficiently long and complex and include capital and lower case letters, numbers and special characters. As an additional precaution, employees should consider changing their passwords before transitioning to remote work.

DO	DON'T
DO create complex passphrases	Do NOT use public or unsecure Wi-Fi networks without using VPN
DO change home Wi-Fi passwords	Do NOT access or send confidential information over unsecured Wi-Fi networks
DO create a separate Wi-Fi network for guests	Do NOT leave electronic or paper documents out in the open
DO install anti-malware and anti-virus software for internet-enabled devices	Do NOT allow family or friends to use company-provided devices
DO keep software (including anti-virus/ anti-malware software), web browsers, and operating systems up-to-date	Do NOT leave devices logged-in
DO delete files from download folders and trash bins	Do NOT select "remember me" on shared devices
DO immediately report lost or stolen devices	Do NOT share passwords with family members
DO log off accounts and close windows and browsers on shared devices	Do NOT use names or birthdays in passwords
DO review mobile app settings on shared devices	Do NOT save work documents locally on shared devices
DO handle physical documents with sensitive and/or confidential information in a secure manner	Do NOT store confidential information on portable storage devices, such as USB or hard drives

Update and secure devices.
To reduce system flaws and vulnerabilities, employers should regularly update VPNs, network infrastructure devices and devices being used to for remote work environments, as well as advise employees to promptly accept updates to operating systems, software and applications on personal devices. When feasible, employers should consider implementing additional safeguards, such as keystroke encryption and mobile-device-management (MDM) on employee personal devices.

Use of personal devices and deletion of electronic files.
Home computers may not have deployed critical security updates, may not be password protected and may not have an encrypted hard drive. To the extent possible, employers should urge employees to use company-issued laptops or sandboxed virtual systems. Where this is not possible, employees should use secure personal computers, and employers should advise employees to create a separate user account on personal computers designated for work purposes and to empty trash or recycle bins and download folders.

Prohibit use of personal email for work purposes. To avoid unauthorized access, personal email accounts should not be used for work purposes. Employers should remind employees to avoid forwarding work emails to personal accounts and to promptly delete emails in personal accounts as they may contain sensitive information.

Secure collaboration tools. Employees and teams working from home need to stay connected and often rely on instant-messaging and web-conferencing tools (e.g., Slack and Zoom). Employers should ensure company-provided collaboration tools, if any, are secure and should restrict employees from downloading any non-company approved tools. If new collaboration tools are required, IT personnel should review the settings of such tools (as they may not be secure or may record conversations by default), and employers should consider training employees on appropriate use of such tools.

Handle physical documents with care. Remote work arrangements may require employees to take sensitive or confidential materials offsite that they would not otherwise. Employees should be advised to handle these documents with the appropriate levels of care and avoid printing sensitive or confidential materials on public printers. These documents should be securely shredded or returned to the office for proper disposal.

Develop clear guidelines and train employees on cyberhygiene. To ensure employees are aware of remote work responsibilities and obligations, employers should prepare clear telework guidelines (and incorporate any standards required by applicable regulatory schemes) and post the guidelines on the organization's intranet and/or circulate the guidelines to employees via email. A list of key company contacts, including Human Resources and IT security personnel, should be distributed to employees in the event of an actual or suspected security incident.

Prepare for remote activation of incident response and crisis management plans. Employers should review existing incident response, crisis management and business continuity plans, as well as ensure relevant stakeholders are prepared for remote activation of these plans, such as having hard copies of relevant plans and contact information at home.

As businesses transition back into the office, incident response, crisis management and business continuity plans, as well as any remote work policies and guidelines, should be reviewed and updated with any lessons learned.

CONTACTS

For more information on Cybersecurity, Privacy and Data, please contact your Katten attorney, the firm's Cybersecurity, Privacy and Data group, or any of the following:

Doron Goldstein
+1.212.940.8840
Doron.goldstein@katten.com

Megan Hardiman
+1.312.902.5488
Megan.hardiman@katten.com

Trisha Sircar
+1.212.940.8532
Trisha.sircar@katten.com

Dagatha Delgado
+1.212.940.6350
Dagatha.delgado@katten.com

Jeremy Merkel
+1.212.940.6339
Jeremy.merkel@katten.com

Katten katten.com

CENTURY CITY | CHARLOTTE | CHICAGO | DALLAS | HOUSTON | LONDON | LOS ANGELES | NEW YORK | ORANGE COUNTY | SHANGHAI | WASHINGTON, DC

Attorney advertising. Published as a source of information only. The material contained herein is not to be construed as legal advice or opinion.

Katten refers to Katten Muchin Rosenman LLP and the affiliated partnership as explained at kattenlaw.com/disclaimer.

3/18/20