ATTORNEYS AT LAW

BULKLEY RICHARDSON

BETTER REPRESENTATION

CYBERSECURITY UPDATE FOR TELEWORKERS

Here we are, approximately nine months into the pandemic, with cases on the rise again and a vaccine on the horizon. Many workers who can work remotely are continuing to do so, and even workers who have returned to a physical office continue to meet on virtual platforms in order to comply with social distancing guidelines.

These remote employees, and the business information to which they have access, are targets of cybercriminals. They are also critical participants in your company's **cybersecurity infrastructure**.

With that in mind, here are a few **reminders** for those conducting business remotely:

- If you are using Zoom, or another online platform, you should use the "waiting room" function and require the use of a password. This should prevent "Zoom-bombing" or other intrusions into your meeting.
- Be suspicious of **emails** that ask you to click on links or download documents, particularly if you are reading email on your phone and cannot view the sender's address.
- If you are using Office365, consider implementing the safeguards, including multifactor authentication, listed **here**.
- Require your employees to encrypt their at-home wireless network by using WPA2/WPA3 options and password protection. Instructions can be found **here**.
- Set up two-factor authentication for access to your company's servers.
- Use a virtual public network (VPN) whenever possible (and train employees to avoid surrendering those credentials to a cybercriminal in an **increasingly common vishing scheme**).
- Always hover over links to confirm that the destination looks to be a legitimate website.

Additional guidance on telework is available from the **National Institute of Standards and Technology**, the **Cybersecurity and Infrastructure Security Agency** and the **Federal Trade Commission**.

If you have questions about implementing these safeguards, or if you would like to update your Written Information Security Program (WISP) to account for a material change in your business environment, please contact a member of Bulkley Richardson's Cybersecurity Team.

Lauren Ostberg

lostberg@bulkley.com
413-272-6282

Jim Duda

jduda@bulkley.com
413-272-6284

Scott Foster

sfoster@bulkley.com
413-272-6258

Sarah Willey

swilley@bulkley.com
413-272-6228