Cybersecurity in the Home Office: How to Stay Vigilant During COVID-19

Amundsen Davis Data Privacy & Security Alert
March 26, 2020

The #1 weakness of a business for cyber security can be users of that technology. From employees to management and those in the C-suite, anyone can fall victim to business email compromise (BEC). That was true when companies had the majority of their workforce in their brick-and-mortar and had control over training and usage under one roof. Now that millions of people are working from home in response to COVID-19 how do businesses prevent cyber security attacks?

Although it's an important precaution to combat the virus, a mass work-from-home directive likely multiplies the challenges of ensuring your workforce is vigilant against BEC and other cyber attacks. Indeed, CISA (the cyber task force for the Department of Homeland Security) has already issued a warning about cyber actors preying on people during these vulnerable times. Threat actors are sending phishing emails posing as legitimate organizations, claiming to offer updates and information about the coronavirus.

What can you do?

1. **Communicate:** Consider sending a reminder and one-page "cheat sheet" reinforcing best practices for using technology at home, including how to avoid BEC. This vigilance can include: (double) checking email addresses; calling the email sender if you still aren't sure about the legitimacy; avoiding click-bate links; refraining from providing personal information (think passwords and account numbers) in response to phone or email solicitation; *ignoring* solicitations for personal information specific to COVID-19 unless you know the sender and/or authenticate the organization before making a donation.
2. **Enforce Password Protection:** Ensure that all of the company's business accounts are protected by strong passwords and user accounts are protected by two-factor authentication (2FA).
3. **Update Software:** Now more than ever encourage employees to keep software updates current and ensure your IT team continues to patch known vulnerabilities.

PROFESSIONALS

Molly A. Arranz
Partner

RELATED SERVICES

Cybersecurity & Data Privacy

4. **Review BYOD Policies:** The BYOD policies your company had in place were meant to protect the company against potential exposure to security risks on personal devices, which can be less secure than corporate devices. Assess how these policies need to be modified now that a majority of your workforce is using their own devices. What are the acceptable uses, supported devices, and security requirements that must be met to access your network and the like?
5. **Check Connectivity:** What, if any, requirements do you have about secure connections to WiFi? Do you have a handle on the security of the connections used by your employees?