Issued 9/13/18

Phished Credentials Caused Twice as Many Breaches than Malware in the Past Year

Personal device use for remote work poses the biggest security risk to organisations safeguarding their increasingly mobile and cloud-based IT environment, according to a new survey of 100 UK-based senior IT security professionals. Conducted from March to May by Rant, the survey found 58% of respondents believe that network access from non-corporate and personally-owned devices such as laptops, desktops or mobile phones is the highest risk in managing remote users, among other findings. 75% of respondents reported that their users now connect remotely to work applications at least 25% of the time. While this remote work trend has created unmatched flexibility and has helped organizations attract top talent globally, it has introduced a major predicament for IT and security teams. This data is underlined by several recent high profile security breaches that originated from third-party suppliers. According to Forrester's 2017 Global Business Technographics Security Survey, 41% of breaches in the past 12 months were incidents within the organization or involved business partners/third-party suppliers. The findings also reveal the extent to which phishing attacks targeting user credentials continue to dominate as the primary source of security breaches, underscoring the need for robust policies around device health and user authentication. When asked about the biggest security incident in the last 12 months that resulted in unauthorized access to corporate applications, nearly half of respondents reported phishing as the cause. The findings reveal:

• Phishing resulted twice as many breaches than malware (48% compared to 22%)

• Phishing resulted in more breaches than malware and unpatched systems combined (48% compared to 41%).

“Outdated devices are particularly vulnerable to being compromised, which can easily spiral into a full-blown, major breach,” Archdeacon added. “Organizations don’t necessarily need to block individuals from using their personal devices, but they do need to re-shape their security models to fit these evolving working practices.”