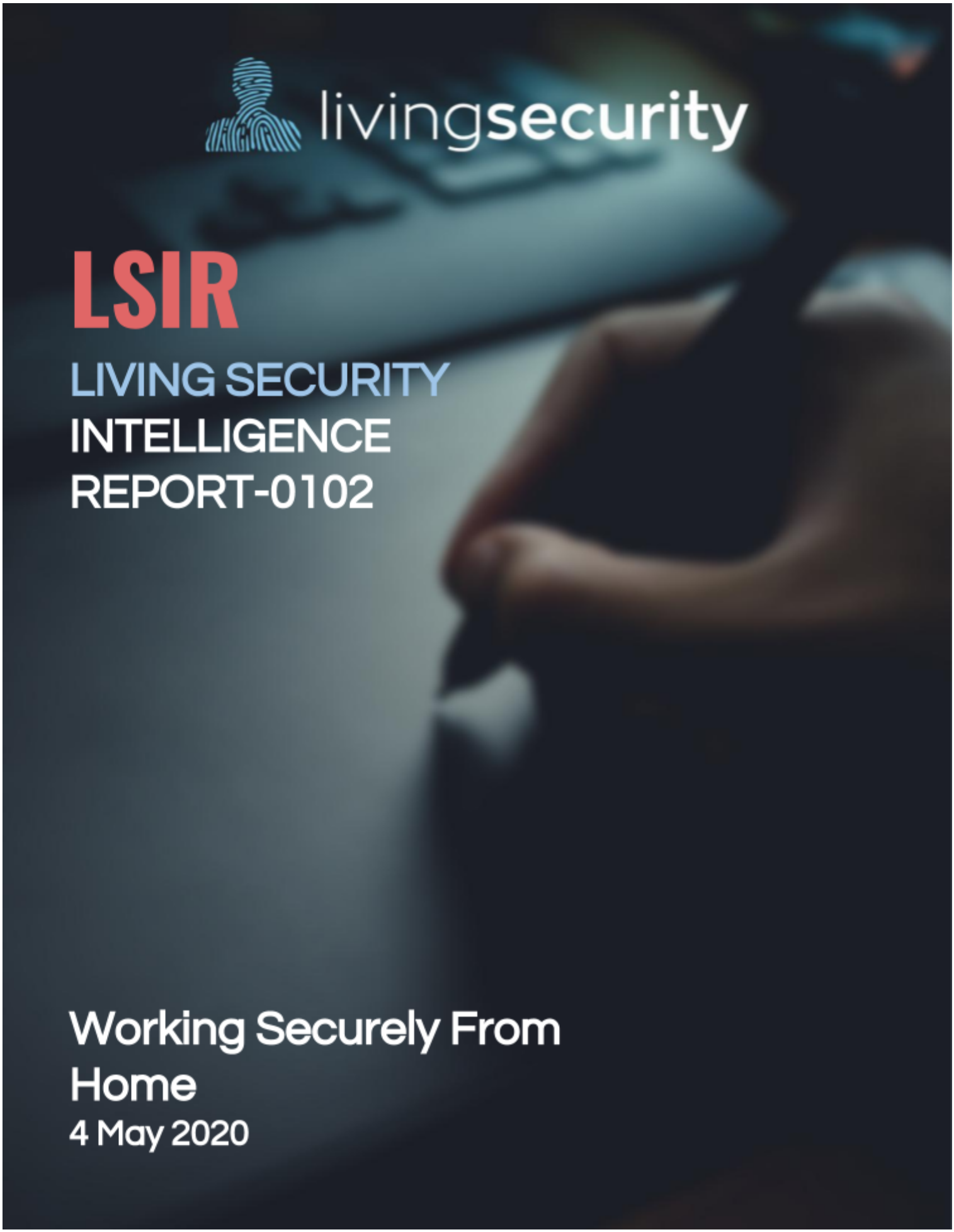
livingsecurity
LSIR
LIVING SECURITY
INTELLIGENCE
REPORT-0102
Working Securely From Home
4 May 2020

Working Securely from Home

Working remotely exposes employees to a range of new cyber threats. Organizations are moving to remote work at a faster rate than ever because of COVID-19 and alongside this push to remote work is an increase in cyber threats targeting a new security perimeter: the employee household.

Since January, 77% of organizations in N. America have moved to remote work. Over this time there has been an 85% increase in phishing attacks, 25% increase in malicious websites and a 17% increase in cyber threats targeting organizations remote access accounts [i]. This is because cyber criminals are adapting to new target areas of weakness. It is *highly likely* that cyber criminals will continue to focus attacks on remote workers and use the panic around COVID-19 to conduct social engineering. It is vital for security awareness program owners and CISOs to understand how new threats affect remote workers because such threats will stay even after businesses return to normal.

Discussion:

Cyber criminals recognize that working remotely is a new experience for many people and are looking to prey on the mistakes that will be made by employees. For example, in order for employees to do their jobs they still need to access work data, and with a lack of understanding about how to protect themselves, remote workers can accidentally expose confidential information. In response, organizations must lay out strict policies on what platforms confidential work information is allowed to be accessed and transferred on. This will help to prevent accidental data breaches and loss of confidential information.

Employees also need to understand the importance of avoiding public Wi-Fi (or neighbors WiFi) when conducting work. When using public Wi-Fi, anyone who is connected to the same network is able to capture your network traffic and use it to steal information and credentials. To prevent this, employees need to check with their IT department to see if they provide VPN connectivity. A VPN will route employees' traffic through their organization's network for additional security.

If a VPN is not provided, then employees need to use trusted home Wi-Fi, Mi-Fi, or LTE with strong passwords when conducting work. This will ensure that the employee has positive control over their network and will be able to prevent strangers from seeing their network traffic.

Personal devices are also at risk of being targeted. Personal devices are 3.5 times more likely to be infected with malware so in order to protect an organization's network it is important for employees to only conduct work on work devices approved by the organization [ii]. By using approved devices, employees can ensure they align with expected updates, security policies, and

procedures.

Cyber criminals are also greatly increasing their efforts in social engineering attacks by using people's fear, anxiety, and curiosity around COVID-19 and remote work as a hook. Human error is involved in 95% of all security breaches, and tugging at people's emotions now is more effective due to the nature of the current pandemic [iii]. It is being used to trick people into clicking malicious email links, visiting malicious websites, and giving away confidential information. To mitigate this issue, employees need to understand the signs of social engineering attacks such as urgency, redirection and unusual requests. By understanding these concepts and reporting suspicious emails to the helpdesk/security team, employees can help decrease the effectiveness of social engineering campaigns.

Another threat that people often do not consider is accidental destruction of work-related material. While working from home lock your workstation and put it away when it's not in use to ensure that no work material is destroyed accidentally by a family member.

Home networks, devices, and public Wi-Fi simply don't provide the same level of security that organizations can. This coupled with common human error and increased susceptibility during COVID-19 while working remotely, positions organizations poorly to defend their new security perimeter.

---

[i] https://www.zscaler.com/blogs/research/30000-percent-increase-covid-19-themed-attacks

[ii] https://threatpost.com/malware-risks-triple-for-remote-workers/154735/

[iii] https://www.csoonline.com/article/3533339/covid-19-social-engineering-attacks.html