Keep Your Network Secure While Working Remotely

During COVID-19

As the COVID-19 pandemic continues to spread throughout the world, an increasing percentage of the workforce will be forced to work remotely in an effort to “flatten the curve” of this deadly virus. In preparation for this massive shift, it’s important to take necessary precautions to protect the networks and systems that store businesses’ private, sensitive data.

In this time of need, the Ingalls Information Security team decided it would be helpful to compile a guide businesses can follow and share best practice measures to ensure secure remote access and business continuity during the COVID-19 pandemic crisis.

Scalability

First, it’s important to identify essential business functions, jobs or roles, and critical elements required to maintain business operations. Your team will need to prioritize remote access for these critical functions. In addition, you’ll likely need to actively source any additional hardware needed for staff members to manage day-to-day operations. If applicable, procure sufficient remote connection licenses and increase bandwidth/firewall/remote access capacity to allow for the added traffic you’ll see once the changes have been made.

Security

Communications on external networks require encryption because they are susceptible to interception and modification. Ensure secure remote access connection by using a Virtual Private Network (VPN). When doing this, you’ll need to make sure you update all VPNs, network infrastructure devices, and devices being used to remote into work environments with the latest software patches and security configurations.

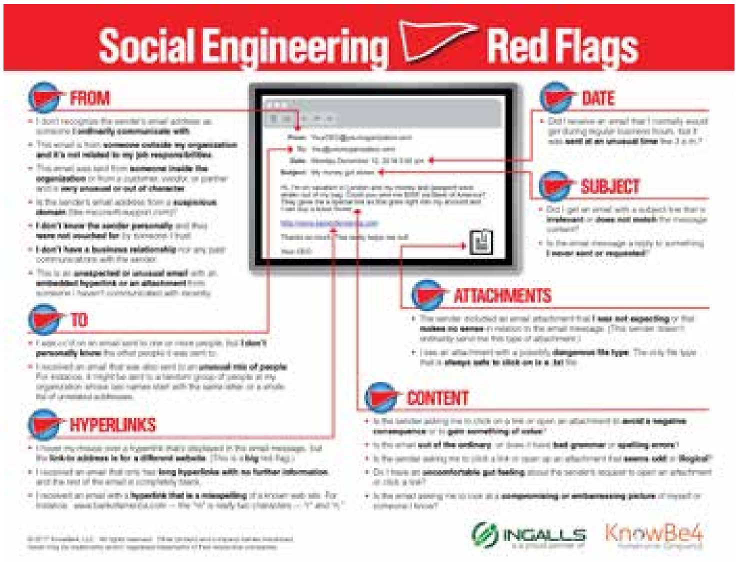
In order to avoid external threats, any remote access to sensitive information by employees or partners should require more than a simple username and password. Secure remote access authentication by enabling multi-factor authentication (MFA). Personally owned devices should be held to the same standard of security as devices on the internal network. Have someone on your team monitor remote access connections for anomalous activity that could be an indicator of compromise (IoC).

Testing & Employee Training

Before you jump into remote work and assume that technology and processes will perform perfectly (they won't), we recommend stress testing your remote capabilities. Go through several phases of tests with a small group to ensure your communication, storage, permissions, backups, and any other critical functions are working properly and remaining secure.

Another aspect of implementing a remote workforce is providing employees instruction on how to remotely access their systems. Ideally, your management or IT department can help create a written document outlining proper procedures and protocols.

Keep your employees on the lookout for signs of social engineering, particularly since fraudulent emails about the coronavirus are likely to increase. These emails (phishing emails) may either have infected attachments or link to malicious websites. Instruct employees to exercise special caution with coronavirus related emails.



Here are a few tips for employees to avoid fraudulent emails:

- If the source of the email sender is unknown do not interact with the email. If the email contains a link, hover over the link to determine the web address of the linked site. See below for additional, detailed Social Engineering Red Flags courtesy of KnowBe4, the market leader in security awareness training and simulated phishing.

  https://www.knowbe4.com/

- Hackers are using malicious coronavirus maps/dashboards to steal information including usernames, passwords, credit card numbers and other data stored in users' browsers. Johns Hopkins has established a legitimate map here.

  https://gisanddata.maps.arcgis.com/apps/opsdashboard/index.html#/bda7594740fd40299423467b48e9ecf6

- Do not reveal personal or financial information in an email, and do not respond to email solicitations for this information.
- Verify a charity's authenticity before making donations.
- Check out these examples of fraudulent COVID emails.

  https://blog.knowbe4.com/piling-on-exploiting-the-coronavirus-for-fraud-and-profit

Questions about how to stay secure while working remotely during COVID-19? Ingalls helps businesses large and small manage security risks and defend against cyberattacks. If you'd like to learn more, please contact us here. One of our cybersecurity experts will be more than happy to assist you and answer any questions you may have.

References

- CISA Insights: Risk Management for Novel Coronavirus (COVID-19)
  https://www.cisa.gov/sites/default/files/publications/20_0306_cisa_insights_risk_management_for_novel_coronavirus_0.pdf

- NIST Special Publication 800-46 v.2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security
  https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final

- CISA Cyber Essentials
  https://www.cisa.gov/cyber-essentials

- CERT/CC: VPN - A Gateway for Vulnerabilities
  https://insights.sei.cmu.edu/cert/2019/11/vpn---a-gateway-for-vulnerabilities.html

- National Security Agency Cybersecurity Advisory: Mitigating Recent VPN Vulnerabilities
  https://media.defense.gov/2019/Oct/07/2002191601/-1/-1/0/CSA-MITIGATING-RECENT-VPN-VULNERABILITIES.PDF

- Telework.gov Guidance
  https://www.telework.gov/guidance-legislation/telework-guidance/security-it/

A Trusted Advisor & Service Provider

Since 2010, Ingalls Information Security has been in the war rooms and board rooms of Global 2000 companies, investigating computer networks targeted and attacked by criminals and nation-state sponsored hackers. This experience gives us an edge in preventing and responding to cyberattacks, as well as developing risk management strategies for our clients. We work for high-profile clients in many different industry verticals, from multi-national conglomerates to small businesses that are increasingly vulnerable to cybercrime.

INGALLS
INFORMATION SECURITY

Cyber Innovation Center (CIC)
6300 Texas Street, Ste. 240, Bossier City, LA 71111

WWW.IINFOSEC.COM
(888) 860-0452