STAYING SECURE WHILE WORKING REMOTELY

IT'S IMPORTANT THAT WE UNDERSTAND HOW TO PROTECT OURSELVES AND OUR BUSINESSES WHILE WORKING REMOTELY, SO WE TOOK THE IMMERSIVE APPROACH TO PROVIDE SOME PRACTICAL ADVICE. WE CAN NOW MAKE ON-LINE CYBER AWARENESS TRAINING AVAILABLE TO YOU.

Recent public health developments mean many workers are now choosing to work, or are being asked to work, from home. More people will need to follow this course of action in the coming weeks, so it's important as a global workforce that we understand how to protect ourselves and our businesses while working remotely.

TYPES OF DEVICE

Perhaps the most important thing to consider is the security of the devices that you are using, as remote working provides attackers with extra opportunities to breach your defences.

Remote workers are likely to connect via two types of device: organizational devices which have been acquired, configured and managed by their organization and 'bring your own' devices which are controlled by the worker. Organizations should also consider how to maintain the security of PC and mobile devices.

TYPES OF THREAT

There are several potential risks that remote working presents to an organization, and it is important to cover all bases. The most prevalent ones are laid out below:

Physical – The organization cannot ensure the physical security of the device, leaving it open to theft or loss. Workers should be encouraged to be vigilant with their devices if working in public places such as coffee shops.

Malware – Malware is malicious software. Remote working can increase the likeliness of this threat, as workers may not be as security-conscious with their own devices as those configured and managed by their organization. This can leave gaps in security for malware to exploit.

Unsecured networks – Remote access is dependent on the Internet, so organizations cannot control the security of networks that remote workers use. These communication systems could be compromised, leaving your sensitive information at risk of being uncovered by malicious actors. Unsecured networks also leave you vulnerable to man-in-the-middle attacks, whereby your communications are intercepted or modified.

Connection of infected devices to internal networks – If a remote worker is using their own malware-infected device and it is connected to an internal network, this malware could spread.

Availability of internal resources to external hosts – Providing external hosts with access to internal servers, particularly from untrusted devices or networks, increases the likelihood that internal servers will be compromised.

The National Institute of Standards and Technology (NIST) recommends assuming that hostile threats exist on external facilities, networks and devices and preparing for remote working based on that assumption. This means a heavy focus in three key areas: keeping remote devices updated, ensuring authentication is effective and securing access from outside corporate networks.

How to protect devices when remote working

Organizations will have to make risk-based decisions about remote access from devices based on the sensitivity of their work. Organizations can consider tiered levels of remote access; this means devices with the most stringent security measures can have the most access, while those the organization has least control over have the least access. It is also important to ensure that sensitive data is encrypted on client devices – or better still, not stored on these devices at all.

Devices used for remote working should have the same levels of security as internal devices. This means ensuring that updates are completed on time, extending patching protocol to these devices, ensuring anti-malware software is installed, and configuring firewalls correctly.

Another thing to consider is network access control, which is authorization based on a type of device and that device's policies. This is known as a security policy enforcement mechanism. Network access control checks can include verifying security patches, checking anti-malware software is functioning and ensuring personal firewalls are operating correctly. See Updates and Patches on Immersive Lab.

Strong authentication is another good step to take to ensure security, and it could take the form of passwords, digital certificates or hardware authentication tokens. Federal agencies use two-factor authentication (2FA) that requires a cryptographic token and password; this measure provides better security than passwords alone.

Introducing periodic re-authentication – for example, after eight hours of a session or 30 minutes idle – can help organizations determine that the person using remote access is authorized to do so. See Multi Factor Authentication Lab.

VPNs create a tunnel between a remote worker's device and an organization's VPN gateway, allowing the remote worker to access computing resources with secure end-to-end. See VPN's and Firewalls Lab.

There are additional modules of learning covered under Work Force Security with specific sections on Cyber Safety and Staying Safe on-line. The full list is shown in the attached Appendix. Note that there are a number of modules designed specifically for managers. Great advice and opportunity to train your employees remotely considering the current situation.

Additional Information

For an idea of the look and feel of the labs, click on the link below;
https://lite.immersivelabs.com/demo?partnerId=CJH-Network

See Short Video here on how the Labs work:
https://www.youtube.com/watch?v=pDwESYNI8Bs&t=2s

For further information contact Colm Hyland at
colmhyland@cjhnetwork.ie

Appendix 1: Immersive labs Awareness Training

Immersive Labs Awareness Training Labs

Workforce Security Training

Cyber Training

What Is Cyber Security?
History of Cybersecurity
Cyber Security Basics
Cyber Terminology
Privacy
Shoulder Surfing
Social Engineering
Disposing of Old Technology
Physical Security
Physical Access Security
Using Your Own Tech at Work
Cybersecurity on The Go

Staying safe on line

Why Cyber Security Is Everyone's Business
Consequences and Impact of Cyber-attacks
Passwords
Antivirus
Malware
Identifying Ransomware
Firewalls and VPNs
Identity Theft
Mobile Security Tips
Backups
Updates and Patches

Knowledge

Cyber 101

Information Security
Why Hackers Hack
Who are the Hackers?
Safe Browsing
Keylogging
Cyber Kill Chain
Cryptocurrency & Blockchain
Darknets
Virtual Card Numbers
Multi-Factor Authentication
Cookies
Geolocation
Fake News

Cyber Investigator

Investigator Operations Security (OPSEC)
Tor and Tor Hidden Services
Domain Intel
Default Credentials
Robots.txt
Reverse Image Search
EXIF
Shodan.io
Cached and Archived Websites
Open Source Intelligence (OSINT): Deleted Tweet
Open Source Intelligence (OSINT): Boarding Pass
Spiderfoot
Analysing Sandbox Reports
Social Media and Privacy

Risk

What Is Risk?
How Is Risk Measured?
Quantitative Risk Measurement
Qualitative Risk Measurement
Asset Inventory and Valuation
Vulnerability Identification
Inherent vs Residual Risk
How to Mitigate Risk
Risk and Control Self-Assessment (RCSA)
Three Lines of Defence
NIST Cyber Security Framework
Security Champions

Compliance

Compliance, Legislation, Regulation and Standards
Policy, Process and Procedure
GDPR Aware
GDPR Aware - Practice
Accreditation
Cyber Essentials
NCSC 10 Steps to Cyber Security
NIS Directive
Payment Card Industry Data Security Standard (PCI-DSS)
Payment Services Directive 2 (PSD2)
Health Insurance Portability and Accountability Act (HIPAA)

Information Technology Health Check (ITHC)
Cloud Security Alliance – Cloud Controls Matrix
What Is ISO 27001?
Cyber Insurance

Infrastructure

Software as a Service (SaaS)
Containers
Infrastructure as a Service (IaaS)
SecDevOps
Infrastructure as Code (IaC)
Security Automation
Platform as a Service (PaaS)
Virtualisation

Cyber for Executives

What is cyber?
Skills Shortage
Incidents
Supply Chains
Whaling
Compliance
Certification
Risk
Unconventional Risk

Cyber for Board Members

Getting Started
Governance
Risk
Awareness
Supply Chain Security
Incidents