MISecure.org

CyberSecurity Remote Connections

TODAY’S TOPIC: Work and Learn at Home Security Checklist

Introductions & Agenda

Brought to you by your friendly partners in K12 Education.

Structure for today:

- Overview of critical concepts for remote working;
- Breakout sessions for group discussion;
- Summary of additional findings to the entire group.

Goal is to provide **practical advice** in a **conducive format** which will be replicated to additional topics.

Keeping Things Practical

Today’s presentation and future webinar sessions tie back to the **Essential Cybersecurity Practices for K12** guide produced by the Michigan K12 community.

These simple concepts need to be **stretched** to include the home environment as much as reasonably possible.

ESSENTIAL

CYBERSECURITY

PRACTICES FOR K12

Transition to Working from Home

- Immediacy caught many by surprise
- Challenges in assigning technology to staff
- Unknown expectations with educating students
- Location-Based Security is Gone
- Personal computing devices must be considered.
- Overload of certain technology components and systems, especially remote access, video conferencing, and cloud.

Basic Security Awareness

Staff must now be extra aware of their environment and surroundings as common protections are **no longer available**.

Staff should be reminded regularly on the following:

- Keep antivirus and antimalware **running** and **updated**.
- Be **extra alert** for phishing and social engineering attacks.
- **Change passwords** to be long and unique if not already.
- **Reach out** to coworkers and IT for any suspicious activity.

What is on your network at home?

Your home is now your secure network boundary.

- Staff **need to know** what is connected on their home networks.
- **Secure** wireless network settings and require a password.
- **Lock** your computer and mobile devices when stepping away.
- Keep **others off** your computer wherever possible.

What is on your network at home?

Utilize resources to protect your newly important home office:

- Securing Your Wireless Network from the Federal Trade Commission
- Charter / Spectrum Support site: Security Awareness
- AT&T: Home network support
- Home Routers:
  - NetGear Support
  - Linksys Support

Providing Software Updates

For organizational-owned machines this may involve a scheduled connection to the VPN and check-in with your management systems.

For home systems, regular and manual checks must be performed.

- For Windows, type **updates** in the Start Menu.
- For Mac, open **Software Updates** from the **System Preferences**.
- For Firefox and Chrome, open the **Menu**, select **Help**, then **About**.

Sending email reminders and setting calendar entries can help greatly.

Protecting Sensitive Data

We now have a duty to protect our data in a much more decentralized manner:

- Utilize **Two-Factor** for IT staff and Data Owners
- Utilize a VPN for **secure access** to internal and ERP resources.
- Investigate **RDP alternatives** such as Citrix, RD Gateway, and Horizon.
- Sensitive data can be stored on an encrypted flash drive using **BitLocker To Go**.

Time for Breaking Out

We will be breaking out into several groups to discuss your successes and challenges in the following areas:

- Basic Security Awareness
  - *How are you making sure staff are computing securely?*
- Keeping Software Updated
  - *How do you manage common and supported software?*
- Protecting Sensitive Data
  - *How are you managing PII and student data remotely?*

We will reconvene in about 15 minutes to share your summary findings with the entire group.

Group Summary Reports

What have been the successes, challenges, and failures in each of these areas:

- Basic Security Awareness
- Keeping Software Updated
- Protecting Sensitive Data

Conclusion

Working and teaching from home is a transformative challenge, and it is alright if we are building the airplane as it is taking off from the runway.

Decentralized computing brings its own challenges, especially when trying to enforce a singular security policy.

Focus on the basics, which will cover a large percentage of the risk.

Keep your ears to the ground and ensure your staff do the same.

MISecure.org

CyberSecurity Remote Connections

Thank You!

Andy Brush, State of Michigan
Merri Lynn Colligan, Washtenaw ISD
Matt McMahon, Gratiot-Isabella RESD
Nicholas Hay, Monroe County ISD
Kevin Hayes, Merit Network
Doug Olson, Traverse Bay Area ISD