
CFMA – Cybersecurity Education and Awareness



- Micro
- mont
- Zoom
- all of
- Cisco
- days o
- Slack
- outbr
- Guess



Windows Defender Browser Protection

! Stop code: Google Chrome Detect Malware | Error Report

Security system has detected the threatening attempt to gain access to your bank logins and related data, but this dangerous connection was blocked with Firewall and further data leak was prevented. We strongly recommend you to perform temporary block of all of your accounts, and take some necessary security measures.

Despite the timely blocking of the connection, there is still a serious threat of private data stealth. Please, don't wait to respond, every minute is important!

There is possibility that virus already hurt your disks or destroyed and stole its data. It is reason for checking current system security and verifying its stability. Do not spend your time and immediately call us or contact our service center support team.

Contact Microsoft Support:
+1 (844) 239-5644

We are waiting for your rapid response to help you. Please contact our administration to solve this issue.

Call Help Desk:
+1 (844) 239-5644

— Remote versus Onsite

- Network Protections
 - Ability to scan for dangerous web requests
- Untrusted LAN
 - Bad guy (or software) on same network
- Disconnected from SecOps
 - Detection and response



— Pockets of Risk

User Behavior	Device and Media
Remote Network	Accounts and Passwords
Physical	Securing Access



- Authorized data flow
- Use of unapproved technology
- Social engineering attacks due to fluidity of processes



— Pockets of Risk

User Behavior	Device and Media
Remote Network	Accounts and Passwords
Physical	Securing Access



- Protections for home network
- Assume compromised network



— Pockets of Risk

User Behavior	Device and Media
Remote Network	Accounts and Passwords
Physical	Securing Access



- Paper records and notes
- Theft or loss of device or media



— Pockets of Risk

User Behavior	Device and Media
Remote Network	Accounts and Passwords
Physical	Securing Access



- Encryption
- Firewall
- Updates (patch, AV)
- Personal Devices



— Pockets of Risk

User Behavior	Device and Media
Remote Network	Accounts and Passwords
Physical	Securing Access

- Passwords
- Multi-factor authentication



— Pockets of Risk

User Behavior	Device and Media
Remote Network	Accounts and Passwords
Physical	Securing Access



- Accessing network
- Accessing applications



— Top Questions to Ask - Business

1. Do you ensure only 'trusted' devices can remotely access network?
2. If there were any rush deployments, have they subsequently been reviewed for cybersecurity concerns?
3. Have devices been properly hardened? Remotely manageable?
4. Has 'acceptable use' guidance been provided to users?
5. What about third party or non-employees?
6. In addition to technical and people risk, does this put at risk our process-based cyber protections?
 - Bank transfer procedures (BEC), contract review, account termination, etc.

— Top Questions to Ask - Workers

1. Am I following established processes?
2. Am I safely managing paper documents?
3. Is my home network secure?
 - Tippy-top question: Do I utilized a guest network for untrusted devices?
4. Am I utilizing company approved hardware and software?
5. Am I aware of company 'acceptable use' policy while working at home?
6. Am I keeping my work stuff separate from my personal stuff?

— Cyber Segue



— Higher Or Lower: 2019 FBI Cyber Stats

Internet Crime Type	Actual Loss
Identity Theft	\$160,305,789
Corporate Data Breach	
Government Impersonation	
Ransomware	
Non-Payment/Non-Delivery	
BEC/EAC	
Tech Support	
Phishing/Vishing/Smishing/Pharming	

— Cyber Security Top Risks

- FBI Top Risks
 - BEC, Ransomware, Tech Support Fraud, Extortion
- Education
 - Cloud Security, DoS, Malware, Phishing, Unsecured Personal Devices
- SMB
 - Phishing, Ransomware, Tech Support Scam, Remote Access Trojan
- Healthcare
 - Breach/Data Leak, Ransomware, Insider Threat

— Top Cyber Risks for Construction Firms

Social Engineering

Ransomware

Wire Fraud

Hacking

— Wire Fraud Tale



1. Real Estate Agent Email Takeover
2. Builder and Builder's Employee Spoofed
3. Fake Wiring Instructions Sent to Buyers from 'builder'
4. Wire Sent to Fraudsters



— Resources

- SANS 'Top 5 Steps to Securely Working from Home'
 - <https://security-awareness.sans.org/sites/default/files/2020-03/02-SSA-WorkingFromHome-FactSheet.pdf>
- FTC 'Online security tips for working from home'
 - <https://www.consumer.ftc.gov/blog/2020/03/online-security-tips-working-home>

— Thank You

- Terry Ziemniak
 - TZiemniak@NorthWonders.com
 - C. 312-834-7621
- North Wonders
 - We provide cyber security strategy and planning services.
 - We offer customized security awareness and training services.
 - www.NorthWonders.com

