UMKC Cybersecurity

Topics

- Stats
- Phishing
- Ransomware
- IS Security Staffing
- Security Operations Center (SOC)
- Computers/Servers
- Security Tools

Stats

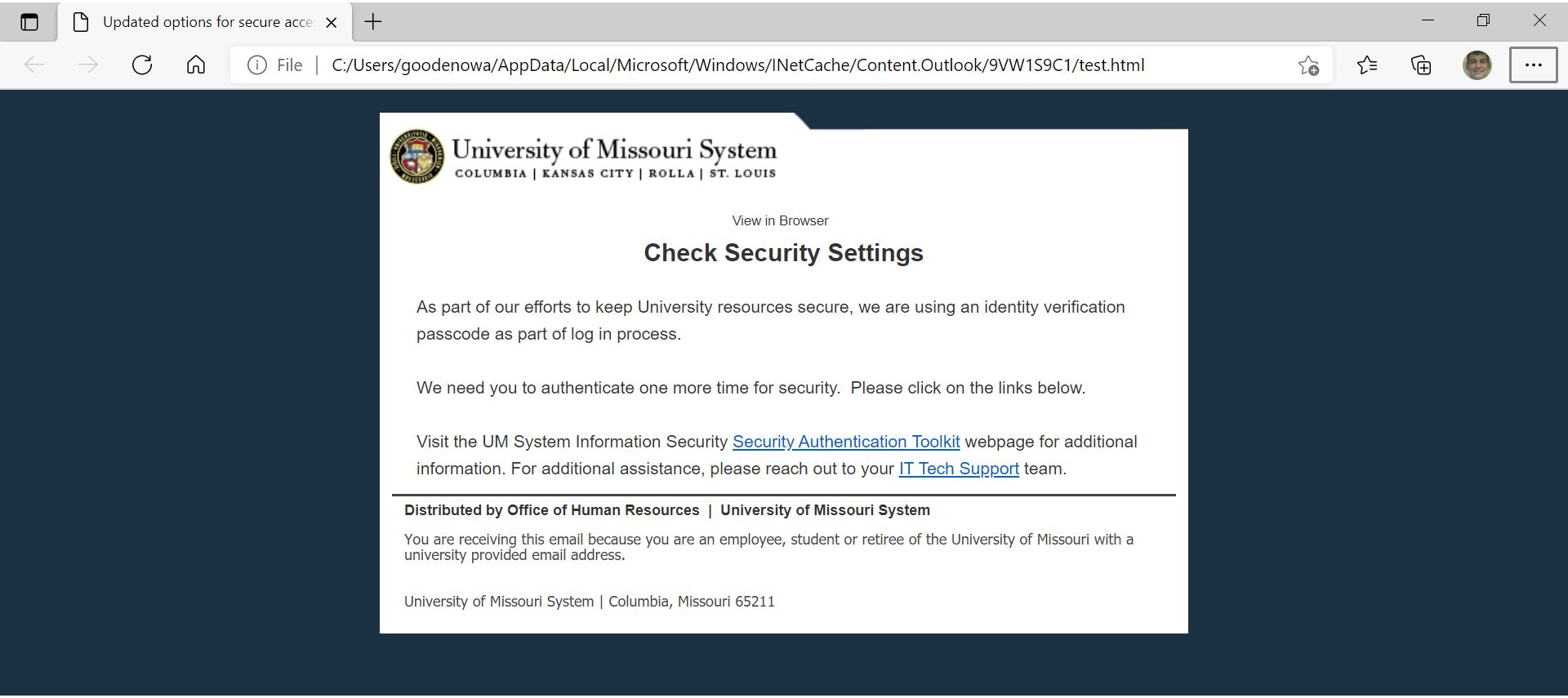
- Higher education is a target for bad actors
- Pre-2010, our first analysis was 9 attempts per second
- June 2017 we filtered out malicious traffic attempts at the following rates:

  373/second, 22,429/minute, 1,345,753/hour, 32,298,079/day

- We switched analysis tools a few years ago. During a random period in April 2020, we had over 36K identified attack attempts.
- Two PDF examples

Phishing

- Email impersonation
  - Gift card scams
- Capture information via a web site after clicking on email links
- UMKC example (next slide)
- UMKC statistics
  - 35.29% of Executive Leadership
  - 14.89% of IT
  - 9.88% was the Academic Unit/Division low
- UM System
  - Annual Security Training
  - New phishing tools from Office 365 (being tested now)



{{.Tracker}}

UMKC

Ransomware

- Not if, but when it will happen
- UMKC has had multiple instances
- UMKC Playbook
- UM System hosted ERP applications
  - Ransom amount
  - Time to restore or rebuild application
  - Lost data
- Scale/Importance of application weighs in decision on how to respond
- Cyberinsurance
- UMKC targeted areas of risk
  - Dentistry, Medicine, Pharmacy, Nursing, Cashiers Office

IS Security Staffing

- Doubled staffing over the past three years
- Additional expertise needed for hardware, security review
- Additional staff with a higher skillset to support compliance needs
  - FERPA
  - HIPAA
  - PCI
  - Controlled Unclassified Information (CUI)
  - Gramm-Leach-Bliley Act (GLBA)
  - National Institute of Standards and Technology (NIST)
    - Cybersecurity standards
    - NIST 800-171
  - Etc.
- Research is a big driver and future staff will be required in this area based on requirements from federal research dollars ($50M threshold)

Security Operations Center (SOC)

- The SOC is a multi-campus security effort that went live in early 2021. Each campus has a staff member work about 2 days a week, handling security incidents that are either reported to the SOC mailbox (sent to the abuse contact at any campus), or which show up as alerts in Office 365 for desktop and Office services.
- Staffed five days a week and on call procedures during the weekend.
- Examples:
  - Compromised accounts
  - Unusual logins outside of the country
  - Spam reports

Computers/Servers

- Every campus computer has a unique administrator password. Hackers can't copy from memory and use it on another machine.
- Administrative rights are removed from all computers for individual users (other campuses in UM system are moving to this policy following)
- Firewalls block machine to machine file sharing. Malware and common worms cannot hop from one compromised workstation to others.
- All Microsoft computers have endpoint protection constantly running and you cannot disable (protected by group policy)
- All servers have required a smart card login for over 15 years (only UM System campus able to institute this)

Security Tools

- Microsoft Advanced Threat Protection software which guards against malicious threats in email messages, attachments, and links
- End Point Protection
- Data loss prevention (DLP) helps you prevent the unintentional or accidental sharing of sensitive information. DLP examines email messages and files for sensitive information, like a credit card number
- Palo Alto Networks
- Cisco

Email Statistics one day last week

- 1,107,660 good emails
- 113,116 blocked at the edge firewall
- 589 advanced phishing filter
- 282 general phishing filter
- 789 ATP generated reputation defender
- ~43K anti-spoofing domain attempts
- 694 malicious URL attempts
- 14 user impersonation attempts

UMKC

Questions/Concerns

- If you want us to run a phishing campaign on your academic unit/division, or
  talk at a lunch session or meeting, or
  need something else

- goodenowa@umkc.edu or x2368

  Technology Support Center x2000