

# Cyber Security Landscape at MSU

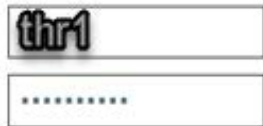
Tom Ritter  
Security and Compliance Officer  
Office of the CIO



**MISSISSIPPI STATE UNIVERSITY**  
INFORMATION TECHNOLOGY SERVICES

# Two – Factor Authentication

Easy To Use – Your Phone Is Your Key



▶ Login as usual



▶ Duo Push, Passcode



▶ Done!



(or tokens / security keys)



# Keystroke Logger



SOFTWARE DEFINED RADIO | PENETRATION TESTING | LOCK PICKS | NETWORKING | ALL PRODUCTS ▾ | BLOG

CART / \$0

INPUT DEVICES

## KeyGrabber

\$40 – \$150

CLEAR

Model

\$150

- 1 +

ADD TO CART



keygrabber-usb-premium-454A5040b-1024

SKU: KD-KeyGrabber-USB-WIFI-Premium

Category: Input Devices

Tags: Device Recording, Penetration Testing



### DESCRIPTION

KeyGrabber products are hardware keyloggers. The keystroke recorder has up to 2GB of memory capacity, stored on a FAT file system. The device is completely transparent from computer operation, and no software or drivers are required. International keyboard layouts are also supported.



**MISSISSIPPI STATE UNIVERSITY**  
INFORMATION TECHNOLOGY SERVICES

# DUO is REQUIRED@MSSTATE

- ▶ If you have access to sensitive university information then you are required to use two factor authentication (2FA) per the Information Security Program [infosecurity.msstate.edu](http://infosecurity.msstate.edu)
- ▶ Population of employees is all Admin Banner users, all users who have access to student information in myBanner
- ▶ Essentially all faculty, most staff and some affiliates except skilled trades
- ▶ ‘Nag’ screen went live Oct 16<sup>th</sup>, 2017
- ▶ <http://duo.msstate.edu>



# Duo Warning Screen

You are required to use two-factor authentication. To comply, immediately enroll at [duo.msstate.edu](https://duo.msstate.edu).

[Continue to myState TEST](#)

For assistance contact the ITS Help Desk:

- Phone (662) 325-0631
- Toll Free (888) 398-6394
- Email [helpdesk@msstate.edu](mailto:helpdesk@msstate.edu)



# Authentication Method



[What is this?](#)

[Need help?](#)

Choose an authentication method



DUO PUSH RECOMMENDED

Send Me a Push



Passcode

Enter a Passcode



Remember me for 24 hours



# Authentication Method

- ▶ Push is recommended via the mobile app
- ▶ Passcodes
  - Generate a passcode from our Duo website
  - Generate a passcode using a token
  - Generate a passcode using the mobile app



# What can a Thief Do with your Personal Information?

- ▶ Open a new checking or credit card account with your SSN
- ▶ Re-route your existing financial statements via a change of address to keep you unaware of activity
- ▶ Get a drivers license in your name with their own photo
- ▶ If a thief gets your password they can change your direct deposit banking information and steal your paycheck or financial aid funds – Yes, this has happened at MSU!!





# Keep Yourself Safe

- ▶ Avoid using easily available information like your birth date, mother's name, phone numbers as PIN or passwords
- ▶ Don't be afraid to ASK WHY your PII (Personally Identifiable Information) is needed
- ▶ Your bank already has it, so why are they asking?
- ▶ Don't leave PII around easily available to roommates/guests/contractors



# Keep Yourself Safe (cont.)

- ▶ Avoid phone scams like the tech support scam where a fake phone support person convinces you or a family member to install malware!
- ▶ Email phishing – opening files from strange email addresses, fake websites that steal a password
- ▶ Shred paper with PII, dumpster diving is low tech but very productive



# What to do if your ID is Stolen

- ▶ Fraud Alert – Contact all three
- ▶ Close accounts when needed
- ▶ File a police report!
- ▶ Use the Federal Trade Commission resources
- ▶ Get credit reports regularly



# IdentityTheft.gov

IdentityTheft.gov can help you report and recover from identity theft.



## HERE'S HOW IT WORKS:



### Tell us what happened.

We'll ask some questions about your situation. Tell us as much as you can.



### Get a recovery plan.

We'll use that info to create a personal recovery plan.



### Put your plan into action.

If you create an account, we'll walk you through each recovery step, update your plan as needed, track your progress, and pre-fill forms and letters for you.



**MISSISSIPPI STATE UNIVERSITY**  
INFORMATION TECHNOLOGY SERVICES

# Credit Freeze vs Fraud Alert

## What's the difference between a credit freeze and a fraud alert?

A credit freeze locks down your credit. A fraud alert allows creditors to get a copy of your credit report as long as they take steps to verify your identity. For example, if you provide a telephone number, the business must call you to verify whether you are the person making the credit request. Fraud alerts may be effective at stopping someone from opening new credit accounts in your name, but they may not prevent the misuse of your existing accounts. You still need to monitor all bank, credit card and insurance statements for fraudulent transactions.

Three types of fraud alerts are available:

- **Initial Fraud Alert.** If you're concerned about identity theft, but haven't yet become a victim, this fraud alert will protect your credit from unverified access for at least 90 days. You may want to place a fraud alert on your file if your wallet, Social Security card, or other personal, financial or account information are lost or stolen.
- **Extended Fraud Alert.** For victims of identity theft, an extended fraud alert will protect your credit for seven years.
- **Active Duty Military Alert.** For those in the military who want to protect their credit while deployed, this fraud alert lasts for one year.

To place a fraud alert on your credit reports, contact one of the nationwide credit reporting companies. A fraud alert is free. The company you call must tell the other credit reporting companies; they, in turn, will place an alert on their versions of your report.



# Proactive Measures to protect campus

- Penetration Testing and State of MS Requirement for an External IT Risk Assessment every three years
- Assessment completed this summer and a remediation plan in place
- Network devices – Printers, Cameras, etc. with username/password of admin/admin....
- Duo Two-Factor Authentication is now required



# NIST 800-171

- Protection standards for Controlled Unclassified Information (CUI)
- Depending on the type of data from the Federal Government CUI could be student financial aid information or research data
- Contract review to ensure that 1) data is classified as CUI and 2) that the university must follow terms of NIST 800-171
- 14 families of security requirements



# **Questions?**

## **General Discussion**

