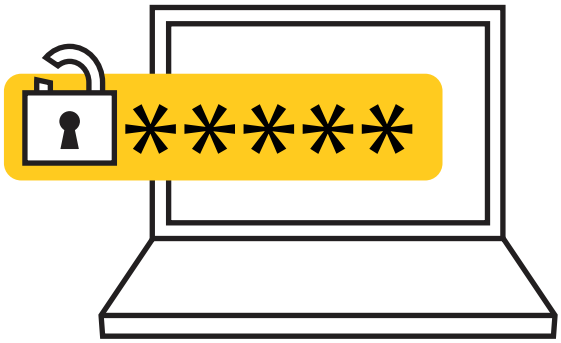

THE
STATE
OF
SECURITY
2016

EMAIL SECURITY & IDENTITY PROTECTION



*The average response time for identifying and shutting down a compromised email account is **under five minutes.***

Reducing Email Threats

Texas A&M's mail relays are capable of processing a massive amount of email. Because of our capacity, cyber criminals want to hack our email accounts. The average response time for identifying and shutting down a compromised email account is under five minutes. This effort protects our reputation and ensures our email services are not blacklisted, allowing communication and research to continue.

This year, Texas A&M IT enabled a new URL-rewriting service, allowing us to dynamically warn and block users from clicking potentially malicious links in emails, even after they have been delivered.

A data loss prevention service will soon be added to the campus mail relays to provide an additional layer of protection from the accidental disclosure of personally identifiable and sensitive information. This service will look for information such as social security numbers or credit card numbers, and will encrypt or quarantine these messages.

IN ONE YEAR

3.9+ BILLION

email deliveries attempted

85%

of emails are **BLOCKED**

EVERY DAY

90K+ PEOPLE

on the network **AT ONCE**

MONITORED 24/7

Strengthening Account Management

Texas A&M IT manages more than 200,000 active accounts, and up to 90,000 accounts may be on the network at any one time.

To monitor vulnerabilities for our large campus population, Texas A&M IT now contracts with SecureWorks to provide security incident and event monitoring 24 hours a day, 365 days a year. This service frees up valuable staff time to assist in incident management and remediation.

*Texas A&M IT works with customers to resolve more than **4,400 security incidents** each year.*

Two-Factor Authentication

To further secure NetID accounts, Texas A&M IT launched NetID Two-Factor Authentication last year. Verifying your identity using a second factor (like your phone or other mobile device) prevents anyone but you from logging in, even if they know your password. The NetID accounts of campus members who have signed up will remain secure even if their password is compromised, with fewer online resources exposed to hackers.

Federal agencies such as the National Science Foundation and the National Institutes of Health have proposed requiring researchers to have this added layer of security. Two-Factor Authentication will help researchers log in more securely with their NetID at federal grant websites and other research resources. Over 5,600 campus members have enrolled 7,000 devices in NetID Two-Factor authentication, using the service an average of 9,000 times per day.

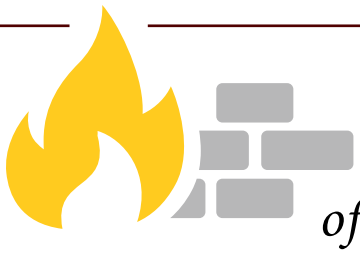
THIS YEAR

5,600+ PEOPLE

ENROLLED IN

NETID TWO-FACTOR AUTHENTICATION

MONITORING THE CAMPUS FIREWALLS, NETWORK & VULNERABILTY



IN 7 MONTHS

13 PETABYTES*

of data **PROTECTED**

**not including IPv6*

Stronger Campus Firewalls

This year, campus bandwidth will increase fivefold from 20G to 100G and a new, next-generation firewall will be deployed to better protect Texas A&M customers and IT resources.

The campus and science DMZ firewalls will also integrate into a single dashboard with 12 new departmental firewalls. This dashboard will provide the Texas A&M IT security team with a comprehensive picture of security across campus.

Expanded Vulnerability Management

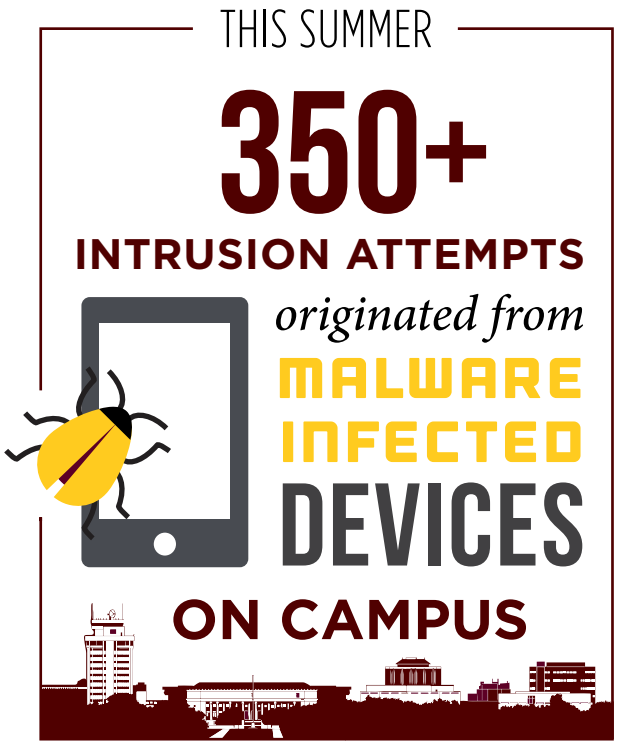
Texas A&M IT recently licensed a vulnerability management solution for 100,000 IP addresses. This service will give campus IT administrators access to a self-service scanning and tracking tool capable of providing customized reports and remediation resources for vulnerabilities detected on their servers and networks.

THIS YEAR

OUR STAFF EARNED

10 NEW CERTIFICATIONS

coming soon:



Improved Network Monitoring

The new Infoblox system has added a Domain Name System (DNS) firewall to the campus network. This system detects and mitigates malware using DNS to communicate with Command and Control Servers and Botnets. If customers try to visit a known malware-infected website, the system will redirect the customer to an informative page and keep their device safe from infection.

If customers try to visit a known-malware infected website, the system will ***block the connection*** *and keep their devices safe from infection.*

Incident & Operations Center

Construction is underway on a state-of-the-art Incident and Operations Center. The center will be used to monitor campus network traffic around the clock, but will be especially valuable during an actual breach or compromise. The center includes a dedicated briefing and response room, secure video conferencing capability, and is designed to allow for flexibility in working with vendors and professionals from across campus.

FOCUS ON EDUCATION & COMMUNICATION

Award-Winning Security Campaigns

Texas A&M IT participates in National Cyber Security Awareness month each year with a campus-wide campaign focused on IT security. Our 2015 campaign, The Game of AggieLIFE, received a national "Best of Category" award from ACM SIGUCCS, a competition that honors the best publications, websites and promotional material produced by university and college IT organizations. Texas A&M IT created this fun, interactive game to educate students, faculty and staff about online security and identity protection. During the two-week campaign, almost 10,000 campus members played the game and BTHO security threats!

*In two weeks, almost **10,000 campus members played** **AggieLIFE** and BTHO security threats!*

Online Presence

Texas A&M IT recently launched a new website, ITSecurityCenter.tamu.edu, focused on sharing security tools, metrics, news and initiatives with the campus community. This website will be a valuable tool for campus IT professionals, updating them on current threats, providing a resource for security best practices and our Google Group communication channel.

IN ONE DAY

TEXAS A&M IT

BLOCKS

10 MILLION SOURCE-BASED

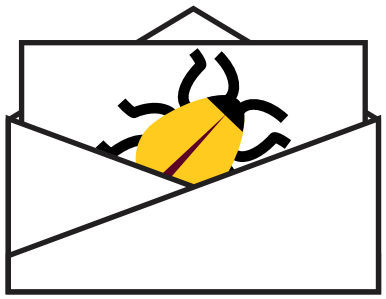
ATTACKS

MONITORS

240,000
ACCOUNTS

190,000
DEVICES

120,000
MAILBOXES



BLOCKS

5.8 MILLION

MALICIOUS EMAILS

ANALYZES & TRIAGES

20,000+
SECURITY EVENTS

Texas A&M IT Security Center

Your first line of defense.

Contact Us

! To report an IT security breach or data release, email ciso@tamu.edu.

? For questions and assistance with compromised accounts, malware infections or other IT security concerns, contact security@tamu.edu.