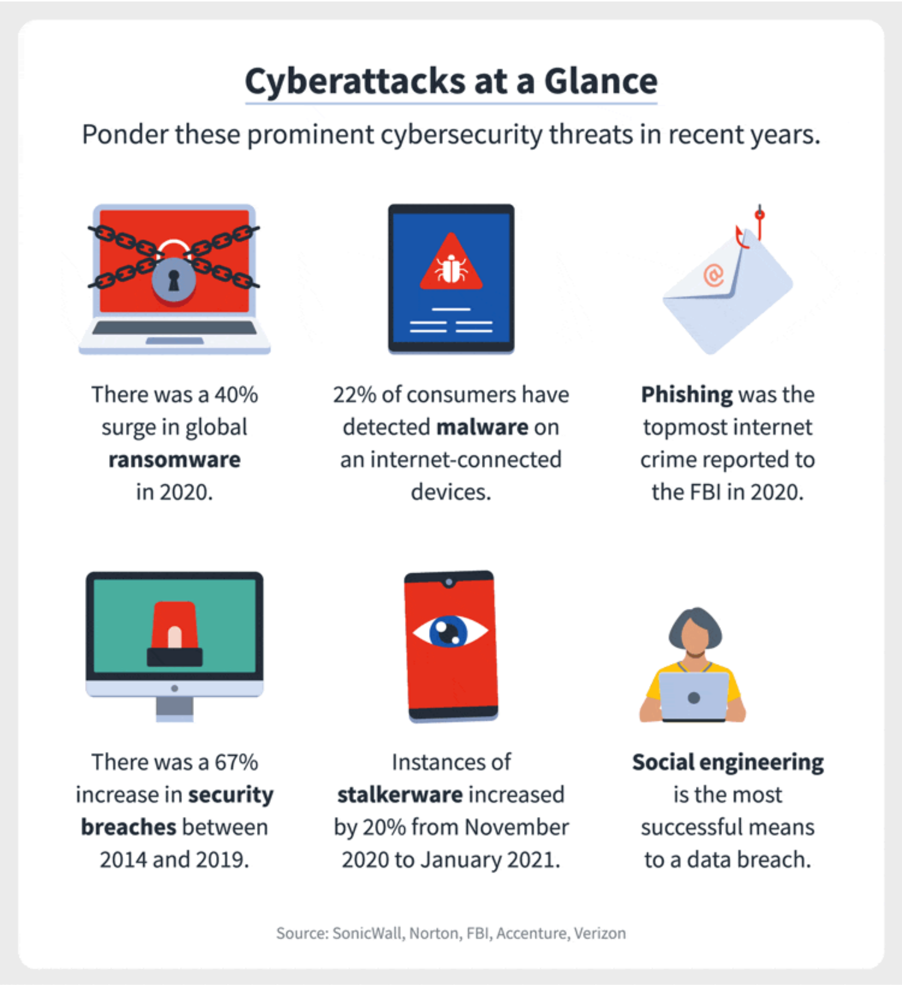
UM Office of Internal Audit

The Audit Perspective

October 2021



Cyberattacks at a Glance

Ponder these prominent cybersecurity threats in recent years.

There was a 40% surge in global **ransomware** in 2020.

22% of consumers have detected **malware** on an internet-connected devices.

Phishing was the topmost internet crime reported to the FBI in 2020.

There was a 67% increase in **security breaches** between 2014 and 2019.

Instances of **stalkerware** increased by 20% from November 2020 to January 2021.

Social engineering is the most successful means to a data breach.

Source: SonicWall, Norton, FBI, Accenture, Verizon

- Breaches result in real cost to the organization. The average cost to the organization is between $100-$148 per compromised record.
- You're more likely to experience a data breach of at least 10,000 records (27.9%) than you are to catch the flu (5-20% according to WebMD).
- Email is the number 1 threat vector used for malware, phishing attacks, and ransomware.

Information Security Controls

According to the University Information Confidentiality/Security Policy, safeguards should be in place to ensure the security and confidentiality of information in offices and data storage areas; identify and protect against anticipated threats to the security or integrity of sensitive or confidential information; and prevent the unauthorized access to, or use of sensitive or confidential information. The department head is responsible for ensuring: 1) an employee is designated to develop and coordinate a departmental information security program, and 2) departmental employees are aware they must adhere to IT policies and are ultimately responsible for ensuring their devices are compliant.

Much of the information in higher education is protected under federal laws. Inadequately safeguarding electronic and physical information could be costly to the University in terms of security breach risks and could lead to significant disruptions in the department's mission.

Sensitive vs Confidential Information

Restricted (sensitive) data is typically subject to specific compliance regulations and based on state or federal laws that are designed to prevent unauthorized disclosure or public release.

Internal (confidential) data is information that is private to UM that could affect institutional operations, reputation, customer privacy, or other affiliates in an undesired manner if it was accidentally disclosed.

See the Information Confidentiality/Security policy for complete definitions.

Ways to Keep UM Information Secure

1. Familiarize Yourself with UM Information Security Policies

Be sure to familiarize yourself with UM Policies including the Information Confidentiality/Security Policy, Anti-Virus Protection for UM Computers Policy, and IT Appropriate Use Policy.

2. Unique Username and Password

All users for each system are required to have their own assigned username with a unique password. Passwords should be a minimum of 8 characters in length, contain capital and lowercase letters, special characters, and numbers. Passwords are never to be shared with anyone.

3. Mobile Device Encryption

All mobile devices (laptops, iPads, external hard drives, etc.) which store sensitive information locally are required to be encrypted. All other mobile devices are strongly recommended to be encrypted.

4. Anti-Virus Protection

All UM systems (servers and workstations) are required to have anti-virus software installed to protect against viruses from the internet or other machines. Symantec is the preferred software and is available for free on the IT website for all University owned computers. Use of any other anti-virus software must be approved by the Chief Information Security Officer (CISO) or Information Security Officer (ISO).

5. Install Updates

Computers are required to be configured to automatically apply application updates and operating system (OS) updates daily.

6. Firewall Protection

A software firewall is required to be enabled on any machine accessing or storing sensitive information. It is strongly recommended for any machine accessing or storing confidential information.

7. Register Systems on the UM System Registry

All UM systems (servers, desktops, laptops, or any electronic device) which store sensitive information locally are required to be registered in the UM System Registry. All UM systems which store confidential information are strongly recommended to be registered in the UM System Registry.

8. 15-minute Session Lock

A password protected session/screensaver lock with a timeout of no more than 15 minutes should be used on all computers to prevent viewing/access of data.

9. Cloud Storage

Only UM-approved services should be used to store University data. See Appendix A in the Information Confidentiality/Security Policy. Additionally, employees should not use a personal Apple ID for UM equipment and the iCloud setting should be disabled.

10. Backup

University departments must have backup practices in alignment with their business continuity management plans. The department must create a backup policy, ensure all employees are made aware of the department's backup policy, and ensure all computers are adequately backed up.

11. Departmental Policy and Procedure Manual

Departments should ensure information security is included in their departmental policies and procedures. Additionally, to help ensure procedures are performed consistently, data is recorded accurately, and new and backup personnel have necessary information to help maintain continuity of operations, the departmental policies and procedures manuals must be regularly (i.e. at least annually) reviewed and updated.

Other Tips to Avoid Becoming an IT Headline

Practice good password hygiene

Use strong and unique passwords on each site and enable multi-factor authentication. Password managers can also be used to easily generate and store secure passwords.

Beware of social engineering tactics

Learn to recognize common methods used by scammers to obtain your personal information, whether via email, text message, phone calls, or in-person. Be skeptical of requests for your personal information or money.

Use only secure WiFi or VPN

Most public or free WiFi networks are unsecure. Always use the Cisco VPN service when connecting to a public WiFi network.

Utilize Checklist Templates

The Office of Information Technology and the Office of Internal Audit have collaborated and created several templates to assist departments:

- Computer Checklist Template – This template assists with setting up new computers but can also be used to ensure current systems are compliant with UM policies.

- UM Information Security Controls Checklist – This template provides an overview of guidance from policies and procedures.

- To assist you in ensuring you're protected, detailed instructions on how to check and/or setup your computer for the above mentioned security controls are available for Windows 10 and Mac.

Security Awareness Training

Departments should work with IT to establish an annual training process. Employees with SAP GUI access and those who handle sensitive information (electronic or physical) are required to complete security awareness training at least annually. It is recommended that all UM employees complete this training. It is the department's responsibility to maintain a list of those who are required to obtain training and retain documentation that training was completed (e.g. copy of the training certificate).

CERTIFICATE OF COMPLETION

UM USER

Security Awareness Training

University of Mississippi

Email Appropriate Use

Official UM email correspondence must originate from a UM email account on the UM Mail (Microsoft 365) servers or a registered, on-campus, or cloud based departmental email server (e.g. username@olemiss.edu). Exceptions include email to support instructional activities, which may originate from UM Gmail (e.g. username@go.olemiss.edu), and extenuating circumstances where access to UM email accounts is limited. Additionally, the IT Appropriate Use Policy states, "*You may not use personal email accounts to conduct official UM business*." Personal email accounts include, but are not limited to, username@gmail.com, username@hotmail.com, username@yahoo.com, etc.

Physical Security of Documentation

Confidential and sensitive information must be kept physically secure. This means, the location of computers, servers, and paper documents must be limited to only the employees who need access to perform their job duties. Physical documentation should be locked in filing cabinets or desks using a key and only those who require access to that information should have a key.

Stop the Scammers: https://news.olemiss.edu/stop-the-scammers-it-shares-best-practices-to-combat-email-fraud/

Learn to Identify Phishing: https://itsecurity.olemiss.edu/phishing-tips

Security Alerts: https://itsecurity.olemiss.edu/alerts

Recent Phishing Messages: https://itsecurity.olemiss.edu/

For assistance with IT Security, employees may contact the IT Helpdesk for support at (662) 915-5222.