Webmail – *A convenience or a data breach just waiting to happen?*

Tom Walsh, CISSP
tw-Security
Overland Park, KS

tw Security
Healthcare Information Security

Background on Webmail

- Employees often do work outside of their office, thus requiring some type of remote access to information resources
- Email is the primary and/or the official communications tool for most organizations
- Therefore, web-based email (webmail) has become one of the most widely used corporate communications resources
- Because of its high value, sensitive nature, and easy access, webmail is often targeted by malicious attackers

Benefits of Webmail

- **Availability**
  - Available on nearly any device with Internet access
- **Convenience**
  - No special software to download; all you need is a web browser
  - For employees or other workforce members
- **Costs**
  - It's free!! (…or is it?)

"The price paid for universal access is a greatly increased attack surface area." - Symantec

The Reality of Today's Cyber World

- **User expectations –**
  - They want access to email at any time, at any location, on any device
- **All it takes is <u>one click</u> by <u>one person</u> to release malicious code**
  - Studies show that more than 20% of email recipients open phishing emails
  - Approximately 12% click on an attachment or embedded link
- **Data leakage is happening – like it or not!**

Introduction – Tom Walsh

- **Certified Information Systems Security Professional (CISSP)**
- **14+ years – tw-Security (formerly: Tom Walsh Consulting, LLC)**
- **Co-authored four books on healthcare security**
  - Published by AMA, AHIMA, and HIMSS (two books)
- **Former information security manager for large healthcare system in Kansas City metro area**
- **Started working in information security in 1992**
- **A little nerdy, but overall, a nice guy ☺**

Webinar Objectives

- **Describe the security issues with making email available anywhere, on any device, at any time**
  - Corporate webmail
  - Personal webmail
- **Understand the forgotten trail of confidential information – "the gift that keeps on giving"**
- **Describe better ways to provide remote access to email**

Terminology

Terminology

- **Breach –** an unauthorized access to protected health information (PHI) as defined by the HITECH Act
- **Cache –** a collection of stored items in a hidden place *(memory)*
- **Certificates** - SSL certificates is an electronic file issued by an authoritative organization to verify that the provider is who they claim to be and indicate secure website connections
- **Cyber –** related to the Internet and computer technology
- **Phishing –** an attempt to acquire key information such as user credentials (User ID and passwords), Social Security number, credit card data, etc. by masquerading as a trustworthy entity *(a form of "social engineering")*
- **Ransomware –** a type of malware that prevents or limits users from accessing their data or system

Terminology – Abbreviations

- **2FA** – Two-factor authentication
- **MDM** – Mobile device management
- **PII –** Personally Identifiable Information (Ex: Social Security Numbers)
- **PHI –** Protected Health Information (Ex: Patient information)
- **URL –** Uniform Resource Locator (used to specify addresses on the World Wide Web/Internet)
- **VPN –** Virtual private network

Risks

Company and personal webmail

Risks – Company Webmail

- **Widespread availability and exposure**
  - Exposure to the outside world increases security risks
  - Easy for cyber criminals to discover the company's webmail address *(See additional slide on this topic)*
  - Once hacked, attackers can read company emails or send email using your company's email account(s)
- **Confidential and sensitive information leaving the controlled confines of your organization's (secure) internal network**

Risks – Company Webmail

- **Local cache (memory storage) of messages and/or attachments to email**
- **Inadequate policies regarding the use of webmail**
  - Both personal and company webmail
- **Failure to secure webmail systems**
  - Webmail servers are Internet facing and at greater risk than internal email servers
- **No digital certificate or a self-signed certificate**

Risks – Company Webmail

- **Webmail address – easy to guess**
  - A web search can be used to discover webmail URL
  - Even if you don't give out your company's webmail address, hackers can guess because many corporate email addresses follow a common pattern, making it easier to guess a user's ID
  - Once cyber attackers have this information, they can employ bots or password crackers (both - automated programs) to guess the correct user password

Risks – Company Webmail

- **Compromised email infrastructure can result in several problems, such as:**
  - Intellectual property loss that can be used for blackmail, or can even be sold on the Internet
  - Email contacts
    - May expose others to future phishing, ransomware, and malware attacks
    - The organization's reputation can be damaged by unintentional phishing or spamming and could lead to the organization being blacklisted

Risks – Using Public Devices

- **Data may be stored in local memory or cache**
- **User forgets to logoff or close the email session**
  - Leaves the website open, allowing unauthorized access unless the system automatically logs users out after a set period of inactivity
- **Keylogger – could capture user credentials or other confidential information**
  - Less likely but similar risk: Shoulder surfing

Risks – Personal Webmail

Allowing your employees to use their personal webmail on your company workstations and network creates additional workplace risks because it bypasses many of the security controls in place on the internal email system

- **Malicious code or email**
  - Can infect your computer systems and network
- **Data Leakage**
  - Sending PHI or PII without encryption
  - Bypassing corporate content filters
  - Forwarding company email to a personal webmail account
  - Using personal webmail as a covert channel for leaking confidential information *(Not being monitored)*

Risks – Personal Webmail

- **Introducing inappropriate content**
  - Bypassing corporate content filters
- **Hacked webmail** (Gmail, Yahoo, and Hotmail)
  - Millions of users' credentials (user IDs and passwords) were taken by hackers
- **User IDs**
  - How many websites use your email address as your unique user ID?

"Email is the skeleton key for all other accounts."
– Troy Hunt, a Microsoft security expert

Risks – Personal Webmail

Q: How does a "free" webmail service make their money?

A: By data mining

- Serving customized ads in their online email client

Q: Anything wrong with that?

A: Any/all email content is now in their databases including: PHI, PII, and other confidential or sensitive information

- Could lead to data breach notifications for unauthorized access to PHI and is there a signed BAA in place?

Solutions

Solutions – Company Webmail

- **Require the webmail account to be locked after five failed logon attempts**
  - Prevents password cracking
- **Limit the number of employees who have access to webmail – only those who really need it**
  - Because of security and HIPAA privacy/breach concerns
  - Use mobile device management (MDM)
  - Make webmail accessible only for internal users
- **Implement two-factor authentication (2FA)**
- **Require the use of a virtual private network (VPN)**

Solutions – Company Webmail

- **Create a policy or update an existing policy to address the expectations for using company webmail**
  - Discourage use of company webmail on public or shared computers (may have keyloggers or other malware installed, or may cache company data)
- **Educate your workforce on the policy and risks associated with remote access to company email**
  - Send periodic reminders
  - Post reminders at the webmail logon pages

Solutions – Company Webmail

- **Ensure server and webmail software are patched with the latest updates**
  - Prevents vulnerabilities from being exploited
- **Monitor access logs for suspicious events**
  - User behavior monitoring with alerts being sent to system administrators
- **Implement an auto logoff timeout that differentiates between:**

  1) a public or shared computer, or

  2) a private computer

Solutions – Company Webmail

- **Prohibit the auto-forwarding of company emails to a personal webmail account**
- **Hide the company webmail page from search engine crawlers**
  - Prevent search engines such as Google, Yahoo, and Bing from returning the company webmail logon page in search results
    - "setting up a robots.txt in the root of your webmail server"
- **Avoid generic or easily guessable webmail URLs**
  - firstname.lastname @webmail.domain.com
  - msmith@mail.domain.com
- **Install a digital certificate from a trusted source**

Case in Point

- **The Syrian Electronic Army's attack on Forbes in April 2014 started with the infiltration of the company's webmail system**
  - They claimed to have taken a million user account names and passwords, according to the group's Twitter feed

Solutions – Company Webmail

- **Require the use of mobile device management (MDM) for remotely accessing company email**
- **Set MDM controls for:**
  - **User authentication** – A passcode, password, or some other means of user authentication

    Note: *For most devices, enabling user authentication automatically encrypts the data stored within the mobile device.*
  - **Automatic lockout** – After a predefined period of inactivity (such as five minutes), a passcode, password, or some other form of user authentication is required to re-enable the device.
  - **Failed Logon Attempts** – Erase the memory of the device after ten failed logon attempts
  - **Block bad apps** – Prevent access to company email if the device has an app installed that used jailbreaking or rooting to install

Solutions – Personal Webmail

- **Secure your password**
  - Use a unique password for your webmail, different from what you use to login on other websites
- **Use two-factor authentication (2FA)**
  - Some webmail systems now support 2FA
- **Secure the devices (workstations, tablets, smartphones) that you use to access webmail**
  - Make sure antivirus software is current and device operating system is patched and updated
- **Consider using a private VPN application**
- **Avoid using public machines to access webmail**

Solutions – Personal Webmail

- **Educate your medical staff on the risks of using personal webmail**
  - Most doctors have a “free” webmail account
  - Make face-to-face presentations at medical staff meetings, especially doctors
  - Send periodic reminders
- **Log out of the webmail and clear the cache memory when finished using webmail**
- **Purchase the business version of webmail**
  - Price is no longer a barrier to having a real tool

(See next slide)

Solutions – Personal Webmail

- **Example: Google Apps business accounts**
  - $5 per user per month, or $50 per user per year
  - Users get a domain name that matches your business; more professional looking than a personal email account
  - Business email includes:
    - Antivirus
    - Anti-spam
    - Anti-phishing
    - Anti-junk mail
    - Encryption (TLS handshake) for inbound and outbound email and forced encryption to all Gmail addresses

Closing Thoughts and Summary

Closing Thoughts

- **Weakest link: The carbon-based interface unit**
- **Complacency leads to breaches**
  "Oh it will never happen to us."
  "The doctors don't put patient information in an email."
  "I can trust my family members not to read my email."
- **The risks associated with webmail now outweigh its convenience**
- **The bottom line: Many companies cannot afford the risks associated with the use of personal webmail inside the corporate network**

Summary

During this webinar, we…

- Described the security issues with webmail – both company and personal webmail
- Provided an overview of the risks, most importantly – data leakage
- Explained safeguards and controls for webmail
- Provided an opportunity to ask questions

Questions?

Recipe for a damaged reputation

1. **Take too much confidential data**
2. **Add one part inadvertent human error or carelessness**

   Note: *You may substitute either a disgruntled employee or a dishonest employee for human error or carelessness*
3. **Mix in too little security, lack of awareness, and/or no accountability**
4. **Allow time for an incident to arise**
5. **Bake under pressure from a public disclosure**
6. **Remove responsible individuals from their jobs**

Congratulations – *Your organization's reputation has been ruined and will become the prime example for others on what not to do!*

Tom Walsh, CISSP

tw-Security

Overland Park, KS

www.tw-Security.com

tom.walsh@tw-Security.com

913-696-1573

tw-Security, a nationally recognized healthcare IT security consulting firm is dedicated to helping healthcare organizations protect their information resources with hands-on experience in creating and managing information security programs.