HC3: Sector Alert

March 1, 2024 TLP:CLEAR Report: 202403010800

Identifying and Mitigating Threats from Fraudulent Websites in the HPH Sector

Executive Summary

Thousands of fradulent websites with links to credential harvesting e-mails or text messages are built every day to try to lure visitors into giving away personal and financial information, buying products that do not exist, or downloading malware that disrupts devices and data. The impact is compounded when it adversely affects victims in the Healthcare and Public Health (HPH) sector, often due to the sensitivity of the data. This threat briefing examines different examples of fake websites, ways to identify and how to report them, and recommendations for how to avoid becoming an accidental victim.

Fraudulent Login Websites Explained

A fake login page is essentially a knock-off of a real login page used to trick people into entering their login credentials, which hackers can later use to break into online accounts. These websites mirror legitimate pages by using company logos, fonts, formatting, and overall templates. Depending on the attention to detail put in by the hackers behind the imposter website, it can be nearly impossible to distinguish from the real thing. Consequentially, fake login pages can be highly effective in their end goal: credential theft.

How do these pages get in front of a consumer in the first place? Typically, scammers will target unsuspecting recipients with phishing emails spoofing a trusted brand. These emails may state that the user needs to reset their password, or entice them with a deal that sounds too good to be true. If the consumer clicks on the link in the email, they will be directed to the fake login page and asked to enter their username and password. Once they submit their information, cybercriminals can use the consumer's data to conduct credential stuffing attacks and hack their online profiles. This could lead to credit card fraud, data extraction, wire transfers, identify theft, and more.

Developing fake login pages is trivial, as many bad actors will sell premade sites for purchase on the dark web. While it has been easier to distinguish between real and fake login pages in the past, criminals are constantly updating their techniques to be more sophisticated, making it more difficult for consumers to recognize their fraudulent schemes.

Examples of Fraudulent Websites

There is no shortage of examples of different types of fake login pages from previous and current successful attempts by scammers, but below are a few notable ones:

- Online stores that advertise incredible deals, but steal payment information or trick visitors into buying fraudulent or nonexistent products.
- Pages that look like the login pages to services or popular websites.
- Sites with malicious pop-ups that can download malware to steal sensitive information.
- Healthcare or health insurance sites that swipe medical data by asking users to verify account information.
- Package delivery websites that ask users to verify their personal information or trick them into giving up their credit card numbers.
- Airfare booking sites that steal personal information like passport or credit card numbers, or sell fake tickets.

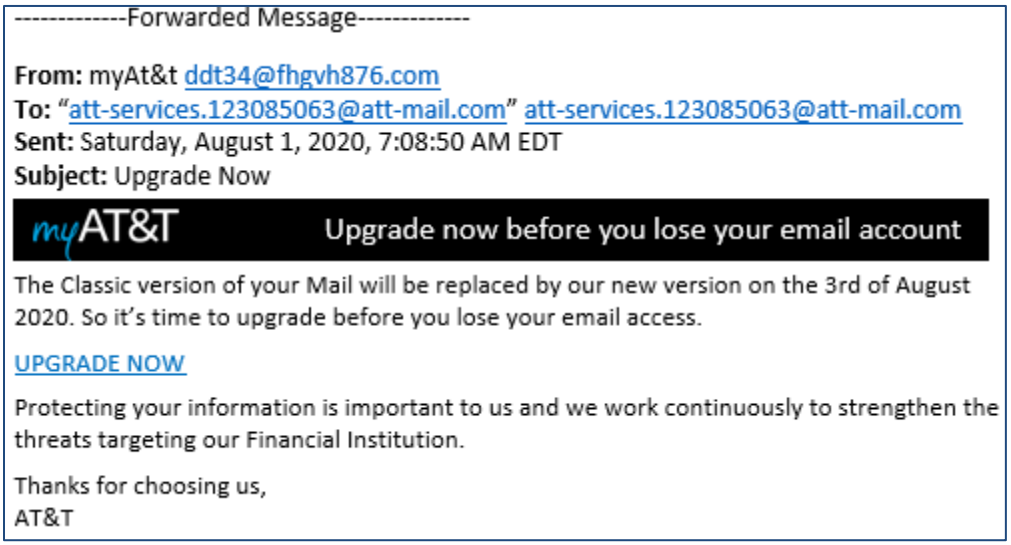
HC3: Sector Alert

March 1, 2024 TLP:CLEAR Report: 202403010800

Identifying Fraudulent Sites

Don't fall for phishing

Most fake login pages are circulated via phishing messages. Always be suspicious of messages that ask for personal details. There are a few ways to determine if it was sent by a phisher aiming to steal identity. Phishers often send messages with a tone of urgency, and they try to inspire extreme emotions such as excitement or fear. If an unsolicited email urges you to "act fast!," slow down and evaluate the situation.



----------Forwarded Message----------

From: myAt&t ddt34@fhgvh876.com
To: "att-services.123085063@att-mail.com" att-services.123085063@att-mail.com
Sent: Saturday, August 1, 2020, 7:08:50 AM EDT
Subject: Upgrade Now

myAT&T Upgrade now before you lose your email account

The Classic version of your Mail will be replaced by our new version on the 3rd of August 2020. So it's time to upgrade before you lose your email access.

UPGRADE NOW

Protecting your information is important to us and we work continuously to strengthen the threats targeting our Financial Institution.

Thanks for choosing us,
AT&T

Figure 1: Example of a phony phishing e-mail posted by AT&T. *(Source: CyberArk)*

Look for misspellings or grammatical errors

Oftentimes, hackers will use a URL for their spoofed website that is just one character off from the legitimate site, such as using "https://www.apple.com" versus "https://www.apple.com." Before clicking on any website from an email asking you to act, hover over the link with your cursor. This will allow you to preview the URL and identify any suspicious misspellings or grammatical errors before navigating to a potentially dangerous website.

https://www.apple.com

https://www.apple.com

Figure 2: Example of a homograph attack by swapping out the "I" in Apple for a "1" or a lowercase "L". *(Source: Identity Guard)*

Look for a closed padlock in the site address bar

Look for a closed padlock or tune icon in the site's address bar that indicates a site has a valid security certificate to block hackers. Scammers can also use certificates to fool visitors into beliving fake sites are real, so it is a good idea to click on the padlock to learn more about the certificate. Information such as registered company name, country of origin, province or state, and locality are signs that the site uses greater security to make it harder to fake.

HC3: Sector Alert

March 1, 2024 TLP:CLEAR Report: 202403010800

Figure 3: Browser padlock icon in site address bar. *(Source: Webopedia)*

Ensure the website is secured with HTTPS

HTTPS, or Hypertext Transfer Protocol Secure, is a protocol that encrypts your interaction with a website. Typically, websites that begin with HTTPS and feature a padlock in the top left corner are considered safer. However, cybercriminals have more recently developed malware toolkits that leverage HTTPS to hide malware from detection by various security defenses. If the website is secured with HTTPS, ensure that this is not the only way you are analyzing the page for online safety.

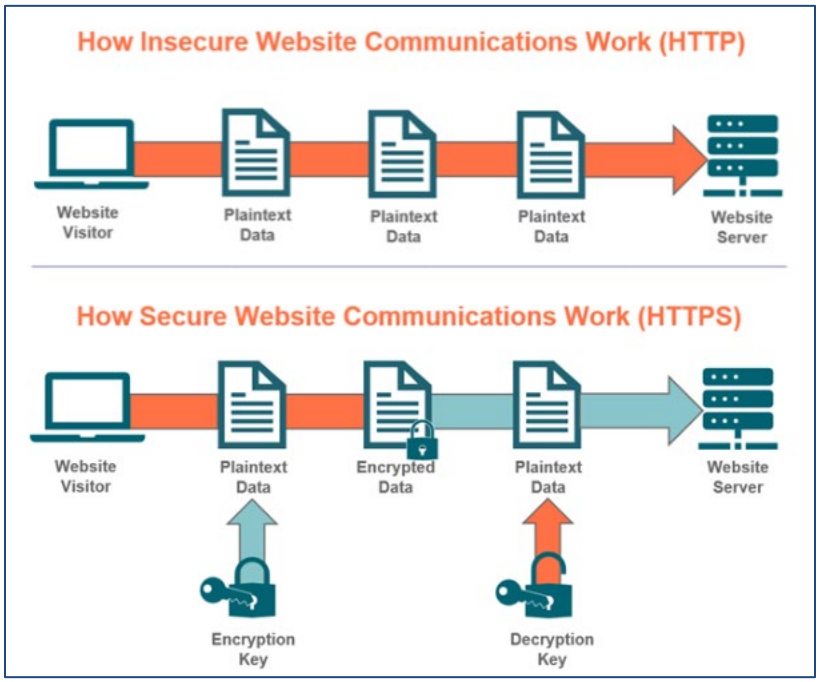


Figure 4: The difference between HTTP and HTTPS connections in terms of protecting data security. *(Source: Savvy Security)*

Enable multi-factor authentication

Multi-factor authentication requires that users confirm a collection of things to verify their identity—usually something they have, and a factor unique to their physical beings—such as a retina or fingerprint scan. This can prevent a cybercriminal from using credential-stuffing tactics (where they will use email and password combinations to hack into online profiles) to access your network or account if your login details were ever exposed during a data breach.

HC3: Sector Alert

March 1, 2024 TLP:CLEAR Report: 202403010800

Figure 5: Examples of multi-factor authentication (MFA) method. *(Source: Externetworks)*

Sign up for an identity theft alert service

An identity theft alert service warns you about suspicious activity surrounding your personal information, allowing you to jump to action before irreparable damage is done.

How to Report Fraudulent Websites

You can report fake websites, e-mails, malware, and other Internet scams to the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3). If you need to report an international scam, report is to the International Consumer Protection and Enforcement Network. Frauds and scams can also be reported to the Federal Trade Commission.

You can also report phishing, fake, or unsafe websites to Google and to Microsoft.

Per the FBI's IC3 reporting standards, gathering as much detailed information as possible on potential or ongoing scams is necessary for an investigation. See below for the types of crimes that they investigate and the essential information needed for each.

Type of Crime	Description	Relevant Information to Report

Business E-mail Compromise	Criminals typically send an email message that appears to come from a business or individual you know—such as one of your business vendors, your organization's CEO, or the title company for your home. The email requests a seemingly legitimate payment, often urgently, via a wire transfer. However, it is all a scam.	- Victim Mailing Address - Victim Email Address - Victim Phone Number - Description of Incident - Victim bank and account details - Subject/recipient bank and account details - Cryptocurrency wallet details (if applicable) - Transaction dates and amounts - The full financial wiring/routing instructions provided by the subject
Ransomware	You are prevented from accessing your computer files, systems, or networks after they are infected with malicious software, or malware. Criminals then demand that you pay a ransom for your files or systems to be unlocked or decrypted.	- Victim Mailing Address - Victim Email Address - Victim Phone Number - Description of Incident - Business name and address - Business IT or remediation firm contact information - Transaction details for any ransom paid - Ransomware variant name (if known); file extension of the encrypted file(s); cryptocurrency type and address; email address utilized by attackers; website(s) / URL(s) provided by attackers; ransom demand amount; whether the ransom was paid and if so, the amount paid
Elder Fraud	Criminals target millions of elderly Americans each year with many different types of financial fraud or confidence schemes, such as romance, lottery, investment, or sweepstakes scams. Criminals may impersonate family members, government agencies, tech support professionals, and others to steal your money and information.	- Victim Mailing Address - Victim Email Address - Victim Phone Number - Description of Incident - Victim bank and account details - Subject/recipient bank and account details - Cryptocurrency wallet details (if applicable) - Transaction dates and amounts - The full financial wiring/routing instructions provided by the subject
Other Cyber Crime	There are many other types of cyber crime that impact both businesses and consumers, including cryptocurrency investment schemes, identity theft, non-payment or non-delivery of merchandise ordered online, credit card fraud, computer intrusions, corporate data breaches, and denial of service website attacks.	- Victim Mailing Address - Victim Email Address - Victim Phone Number - Description of Incident - Any additional information requested in the form deemed relevant to your report

MITRE ATT&CK Techniques

HC3: Sector Alert

March 1, 2024 TLP:CLEAR Report: 202403010800

MITRE ATT&CK framework is a globally accessible knowledge base of adversary tactics and techniques designed for threat hunters, defenders, and red teams to help classify attacks, identify attack attribution and objectives, and assess an organization's risk. While not exclusive, below are some sample MITRE ATT&CK techniques that have been used by threat actors relevant to this problem set:

Phishing	
ID: T1566	
Sub-Techniques	
T1566.001	Spearphishing Attachment
T1566.002	Spearphishing Link
T1566.002	Spearphishing via Service
T1566.004	Spearphishing Voice
Description	
Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., Email Hiding Rules). Another way to accomplish this is by forging or spoofing the identity of the sender, which can be used to fool both the human recipient as well as automated security tools. Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,[5][6] or install adversary-accessible remote management tools onto their computer (i.e., User Execution).	

Phishing for Information	
ID: T1598	
Sub-Techniques	
T1598.001	Spearphishing Service
T1598.002	Spearphishing Attachment
T1598.003	Spearphishing Link
T1598.004	Spearphishing Voice
Description	
Adversaries may send phishing messages to elicit sensitive information that can be used during targeting. Phishing for information is an attempt to trick targets into divulging information, frequently credentials or other actionable information. Phishing for information is different from general Phishing in that the objective is gathering data from the victim rather than executing malicious code. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the	

adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass credential harvesting campaigns.

Adversaries may also try to obtain information directly through the exchange of emails, instant messages, or other electronic conversation means. Victims may also receive phishing messages that direct them to call a phone number, where the adversary attempts to collect confidential information.

Phishing for information frequently involves social engineering techniques, such as posing as a source with a reason to collect information (ex: Establish Accounts or Compromise Accounts) and/or sending multiple, seemingly urgent messages. Another way to accomplish this is by forging or spoofing the identity of the sender, which can be used to fool both the human recipient, as well as automated security tools.

Phishing for information may also involve evasive techniques, such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., Email Hiding Rules).

Phishing (Mobile)
ID: T1660
No Sub-Techniques
Description
Adversaries may send malicious content to users in order to gain access to their mobile devices. All forms of phishing are electronically delivered social engineering. Adversaries can conduct both non-targeted phishing, such as in mass malware spam campaigns, as well as more targeted phishing tailored for a specific individual, company, or industry, known as “spearphishing”. Phishing often involves social engineering techniques, such as posing as a trusted source, as well as evasion techniques, such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages. Mobile phishing may take various forms. For example, adversaries may send emails containing malicious attachments or links, typically to deliver and then execute malicious code on victim devices. Phishing may also be conducted via third-party services, like social media platforms. Mobile devices are a particularly attractive target for adversaries executing phishing campaigns. Due to their smaller form factor than traditional desktop endpoints, users may not be able to notice minor differences between genuine and phishing websites. Further, mobile devices have additional sensors and radios that allow adversaries to execute phishing attempts over several different vectors, such as SMS messages, Quick Response (QR) Codes, and Phone Calls.

The Way Forward

In addition to a HC3 Analyst Note on Healthcare Sector DDoS Guide on how to safeguard against ransomware/extortion attacks, some cyber security professionals advise that the healthcare industry acknowledge the ubiquitous threat of cyberwar against them and recommend that their cybersecurity teams implement the following steps:

- Educate and train staff to reduce the risk of social engineering attacks via email and network access.

- Assess enterprise risk against all potential vulnerabilities and prioritize implementing the security plan with the necessary budget, staff, and tools.
- Develop a cybersecurity roadmap that everyone in the healthcare organization understands.

At no cost, the Cybersecurity & Infrastructure Security Agency (CISA) also offers Cyber Hygiene Vulnerability Scanning services to federal, state, local, tribal and territorial governments, as well as public and private sector critical infrastructure organizations. This service helps organizations monitor and evaluate their external network posture.

The probability of cyber threat actors targeting the healthcare industry remains high. Prioritizing security by maintaining awareness of the threat landscape, assessing their situation, and providing staff with tools and resources necessary to prevent an cyberattack remains the best way forward for healthcare organizations.

Relevant HHS Reports

HC3: Analyst Note – Healthcare Sector DDoS Guide (February 13, 2023)

HC3: Analyst Note – Vishing Attacks on the Rise (August 19, 2022)

HC3: Threat Briefing – Cybersecurity Incident Response Plans (October 12, 2023)

HC3: Threat Briefing – Data Exfiltration Trends in Healthcare (March 9, 2023)

HC3: Threat Briefing – The Impact of Social Engineering on Healthcare (August 18, 2022)

HC3: Threat Briefing – Multi-Factor Authentication & Smishing (August 10, 2023)

HC3: Threat Briefing – Strengthening Cyber Posture in the Health Sector (June 16, 2022)

HC3: White Paper – AI-Augmented Phishing and the Threat to the Health Sector (October 26, 2023)

HC3: White Paper – QR Code-Based Phishing (Quishing) as a Threat to the Health Sector (October 23, 2023)

References

Beal, Vangie. “Browser Padlock Icon.” Webopedia. September 9, 2021. https://www.webopedia.com/definitions/padlock-icon/

“Fraudulent Websites.” U.S. Army Cybercommand. Accessed February 29, 2024. https://www.arcyber.army.mil/Resources/Fact-Sheets/Article/3301745/fraudulent-websites/

“How to Spot Fake Login Pages.” McAfee. Accessed February 29, 2024. https://www.mcafee.com/learn/how-to-spot-fake-login-pages/

“HTTP vs HTTPS Security: The Differences Between These Protocols.” Savvy Security. March 30, 2021. https://cheapsslsecurity.com/blog/http-vs-https-security-the-differences-between-these-protocols/

"Internet Crime Complaint Center (IC3)." Federal Bureau of Investigation. Accessed February 29, 2024. https://www.ic3.gov/Home/ComplaintChoice

"Multi-Factor Authentication (MFA): Strengthening Your Online Security." Externetworks. Accessed February 29, 2024. https://www.extnoc.com/learn/security/multi-factor-authentication

"Phishing Attack." CyberArk. Accessed February 29, 2024. https://www.cyberark.com/what-is/phishing/

Toohil, Ryan. "How To Tell If a Website Is Fake: 12 Warning Signs." Identity Guard. February 21, 2024. https://www.identityguard.com/news/how-to-tell-if-a-website-is-fake

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback