National Cybersecurity Awareness Month

National Cybersecurity Awareness Month

OCTOBER 2017 WEEK 2

Cybersecurity in the Business Section

The IHS Explainer

2017 IN REVIEW HEALTHCARE BREACHES

The healthcare sector has a lot of information that can be valuable to criminals and thus it is an attractive target. Healthcare organizations often have personal information that criminals can use for traditional financial fraud -- things like names and Social Security numbers. Such organizations also have health insurance information, which can be more valuable because malicious actors can use it to commit medical fraud such as obtaining free medical care, purchasing medical equipment, or acquiring payment for fraudulent services.

Many breaches were in the news in 2017, which resulted from exposed websites, unencrypted storage drives, and users falling for phishing schemes.

This article highlights some of the largest healthcare breaches that occurred in 2017 and some key points that will help you do your part to make sure Indian Health Service (IHS) is safeguarding patients' information so we don't make the news for the wrong reasons!

RANSOMWARE. The Women's Health Care Group of Pennsylvania notified 300,000 patients that a ransomware attack had put their personal health information at risk. The clinic discovered in May that a server and workstation located at one of its offices had been "infected by a virus designed to block access to system files."

IHS Tips. Early warning signs of a potential malware infection include: emails, text messages, or other types of peer-to-peer messages indicating you won something or owe a payment; computers running slower than usual; and unusual or new types of pop-up windows showing up.

PHISHING ATTACK. UC Davis Health notified 15,000 patients of a security breach after an employee fell prey to an email phishing scam and disclosed login credentials. The cybercriminal used these credentials to send emails to other staff members and requested bank transfers for large sums of money.

IHS Tips. Think before you click! Hover over links that you are unsure of before clicking on them, and pay attention to the website's URL. A malicious website may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com versus .net). Phishers like to use scare tactics and may threaten to disable an account or delay services until you update certain information.

(CONTINUED ON PAGE 2)

2017 IN REVIEW HEALTHCARE BREACHES

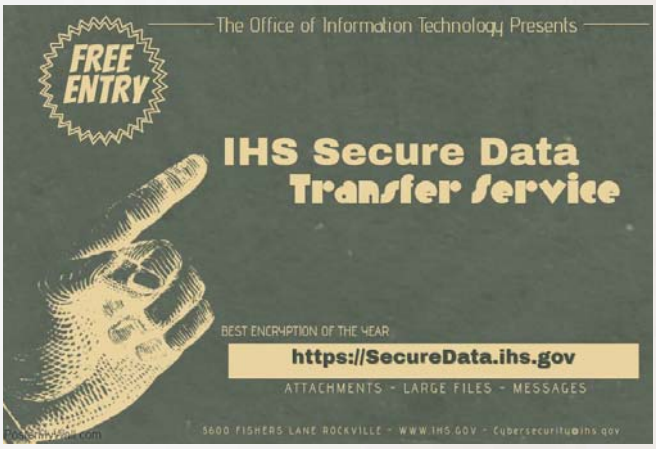
(CONTINUED FROM PAGE 1)

STOLEN HARD DRIVE. A hard drive containing the personal data of about 1 million people was stolen from Washington State University in April. The hard drive contained backup files that included Social Security numbers and personal health data.

IHS Tips. If you are backing up sensitive information such as protected health information, contact your local IT staff or Area Information System Security Officer (ISSO) to make sure you are doing it correctly. And remember: sensitive data stored on mobile devices and portable media requires that: 1) you have a business need; 2) you have authorization; 3) the device is properly encrypted; and 4) the device is physically secured when not in use.

STOLEN LAPTOP. Providence-based Lifespan notified about 20,000 patients that a laptop theft may have exposed their sensitive information. The health organization said an employee's MacBook was taken during a car break-in. The computer was unencrypted and was not password protected.

IHS Tips. A minor distraction is all it takes for a laptop to vanish. Treat your laptop like cash. Consider carrying your laptop in something less obvious than a laptop case. Don't leave your laptop unattended, and don't keep passwords with your laptop or in its case.



AS AN IHS EMPLOYEE, YOU ARE A BIG FISH!

Cyber attackers are using new hooks called spear-phishing to disguise their targeted attacks. They research organizations online to learn all they can, including employee names, phone numbers, and email addresses. They continue their data gathering on social media sites like LinkedIn, Facebook, and Twitter. With this information they bait the perfect hook with an emotional trigger such as authority, fear, reward, or curiosity. Then, they send you an email pretending to be a real person, often using the organization's logo or official email signature.

These emails are extremely realistic-looking and hard to detect because they appear to come from someone you know or work with. The email urgently asks you to take an action that bypasses standard security practices, like providing sensitive data to unverified recipients or logging in to an unconfirmed webpage. Their careful reconnaissance work can snag a really big fish because such emails don't contain malicious attachments or links or other red flags that tip off security technologies like anti-virus or firewalls. No matter the hook – the cyber criminal's goal is the same – to rush you into making a mistake.

REPORT PHISHING EMAILS

If you become the fish on the hook, take a deep breath and report it immediately. In the same way a fish can stay alive out of water for a few minutes, you have a few minutes to potentially survive a phishing disaster unscathed!

Don't think that just closing the browser page will make it go away. You can't throw this phish back! *You must report it!*

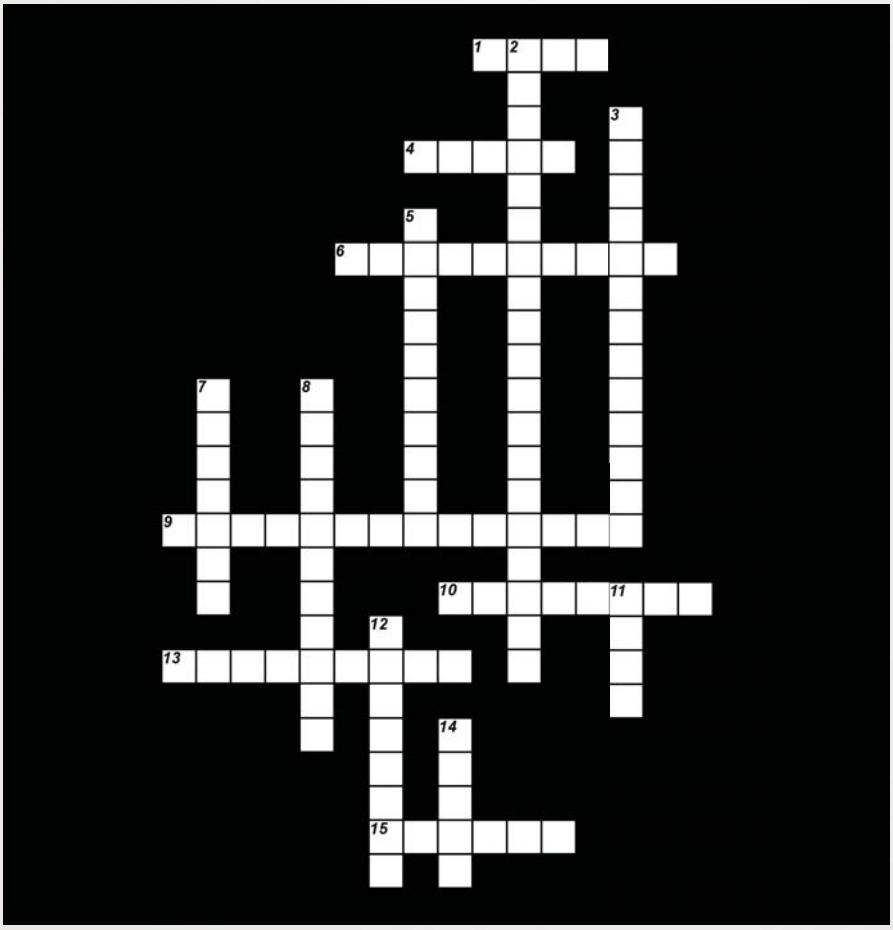
To report phishing emails, contact your local ISSO or the IHS Cybersecurity Incident Response Team (CSIRT) at CSIRT@IHS.GOV.

FREE WI-FI

Public Wi-Fi connections are available at more and more places. Everywhere from hotels to fast food restaurants to even retail outlets offer free Internet connectivity. The concern with these free hotspots is that users cannot know the level of security that the providing host has in place, and therefore cannot know who may be watching the data being transmitted.

Watch those web addresses – Any time you're connecting in public, it's a good idea to avoid websites that don't have an HTTPS or SSL designation in the address at the top of the screen. Using secured web addresses lets you take advantage of both your protective measures and the ones that the websites have in place.

Avoid logging into sensitive accounts – Must you check your online banking account from the coffee shop, or could it wait until you are on a secure network? Unless it's absolutely necessary to log into sensitive accounts, such as your bank or credit card account, save the important web surfing for when you're back on your own secured network.



Across

1. Wireless network.
4. Electronic messages.
6. The organized provision of medical care to individuals or a community.
9. Any government system that provides monetary assistance to people with inadequate or no income.
10. Attempting to steal information through social engineering.
13. Self-contained electronic storage device.
15. Portable computer.

Down

2. Agency providing federal health services to American Indians and Alaska Natives.
3. Protections against the unauthorized or criminal use of electronic resources.
5. Malware that demands payment.
7. Interconnected computers.
8. Apps and websites that let users share personal information.
11. One appointed by IHS to ensure the security of IT resources (acr.).
12. Device or system that blocks unauthorized network access.
14. Secure form of Hypertext Transfer Protocol.

JOKE OF THE DAY:
My brother is in a band named 998MB...
but they never made a gig!

Answers

1. Wi-Fi. 2. Indian Health Service. 3. Cybersecurity. 4. Email. 5.Ransomware. 6. Healthcare. 7. Network 8. Social media. 9. Social security. 10. Phishing. 11. ISSO. 12. Firewall. 13. Hard drive. 14. HTTPS. 15. Laptop.