The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE..

- What Is Encryption?
- Encryption at Rest
- Encryption in Transit

Encryption

What Is Encryption?

You may hear people use the term "encryption" and how you should use it to protect yourself and your information. However, the concept of encryption can seem confusing. In addition, encryption cannot protect you from everything; it has its limitations. In this newsletter, we explain in very simple terms what encryption is, why you should use it and how to implement it properly.

Guest Editor

Christopher Crowley(@CCrowMontance; +ChrisCrowley) is a consultant based in the Washington, DC area. He is the lead instructor of the SANS Institute course Mobile Device Security and Ethical Hacking (SEC575), as well as the author of Incident Response Team Management (MGT535).

You have a tremendous amount of sensitive information on your devices, such as financial documents, pictures, email and medical records. If you were to have one of your devices lost or stolen, all of that very sensitive information could be accessed by whoever possesses it. In addition, you may conduct sensitive transactions online, such as online banking or shopping. If a cyber attacker were to monitor your online activities, they could steal all of your information, such as your financial account or credit card numbers. Encryption protects you in these situations by ensuring unauthorized people cannot access or modify your information.

When information is not encrypted, it is called plain text. This means anyone can easily read or access it. Encryption converts this information into a non-readable format called cipher text. Encryption works by using complex mathematical operations and a unique key to convert your information into cipher text. The key is what locks or unlocks your information, just like a key locks or unlocks a door. A common example of a key is a password. Only people who have that password can decrypt and access your information. To protect your encrypted information, you need to protect your key. In general, encryption works in two ways: you can encrypt data at rest (such as the data stored on your laptop) or data in motion (such as transmitting information online).

Encrypting Information at Rest

The primary goal of encryption at rest is to protect information in case your computer or mobile device is lost or stolen. This was not an issue fifteen years ago, as most computers were big, clunky devices that were very difficult to move

© The SANS Institute 2014

Encryption

around. Today, many laptops weigh only a few pounds, while a mobile device can weigh mere ounces. These devices are extremely powerful and hold a tremendous amount of information, but they are also very easy to lose. In addition, other types of mobile media can hold sensitive information, such as USB flash drives or CD-ROMs. A common technique for encrypting information on these storage devices is called Full Disk Encryption (FDE). This means that everything on the system is automatically encrypted; you do not have to decide what or what not to encrypt. Most operating systems nowadays come with Full Disk Encryption built in; you simply have to enable it. For example, Mac OS X includes FileVault, while some versions of Windows include Bitlocker. If your computer supports Full Disk Encryption, we highly recommend you enable it. In addition, most mobile phones support Full Disk Encryption for their internal storage devices. For example, iOS, the operating system for iPhones and iPads, automatically applies Full Disk Encryption once a passcode has been set. To learn if your work computer or mobile device supports Full Disk Encryption, ask your help desk or supervisor. For your personal computers, contact your computer manufacturer or review the online documentation.

Encryption is a powerful way to secure your information, but it is only as strong as your key.

Encrypting Information in Transit

Information is also vulnerable when it's in transit. If the data is not encrypted, it can be monitored and captured online. This is why you want to ensure that any sensitive online communications, such as online banking, sending emails and even accessing social media sites, are encrypted. The most common type of online encryption is HTTPS. This means all traffic between your browser and a website is encrypted. Look for https:// in the URL, a lock on your browser or your URL bar turning green. These are all signs that the communication is encrypted. Depending on your browser and the website, you may see all three at the same time. In addition, whenever you connect to a public Wi-Fi network, be sure to use encryption whenever possible. Finally, when sending or receiving email, make sure your email client is set up to transmit your email over an encrypted channel. Most email clients provide encryption. In addition, your ISP may be able to help you enable encryption on your email client.

© The SANS Institute 2014

Implementing Encryption Properly

Regardless of which type of encryption you are using or how you use it, almost all forms of encryption share some common steps for using it properly:

- Your encryption is only as strong as your key. If someone guesses or compromises your key, they will have access to your data. You need to protect your key.
- If you are using a passcode or password for your key, make sure it is long, secure and that you do not lose or forget it. If you forget it, you will be locked out of your own data.
- Your encryption is only as strong as the security of your computer. If your computer has been compromised or is infected, cyber attackers can bypass your encryption. As such, be sure to keep your computer or mobile devices secure as well.
- If you are provided different options for encryption, always choose the strongest method.

HEALTHCARE AWARENESS TRAINING

The Healthcare industry is quickly evolving as it moves away from paper records and towards electronic health records (EHRs) and mobility-based services. These changes present new risks and responsibilities associated with protecting healthcare data. While HIPAA helps to define new regulations surrounding these issues, we must also do our part to ensure that all employees are educated about what this means for them in their roles. Check out SANS Securing The Human's new awareness program designed specifically for healthcare organizations by visiting http://www.securingthehuman.org/info/162782.

Resources

Mac OS X FileVault:	http://support.apple.com/kb/ht4790
iOS Encryption:	http://support.apple.com/kb/ht4175
Android Encryption:	http://www.androidauthority.com/how-to-encrypt-android-device-326700/
Windows Encryption:	http://windows.microsoft.com/en-us/windows/protect-files-bitlocker-drive-encryption#1TC=windows-7
Securing Your Computer:	http://www.securingthehuman.org/ouch/2012#december2012
Password Managers:	http://www.securingthehuman.org/ouch/2013#october2013

License

OUCH! is published by SANS Securing The Human and is distributed under the Creative Commons BY-NC-ND 3.0 license. You are free to share or distribute this newsletter as long as you do not sell or modify it. For past editions or translated versions, visit www.securingthehuman.org/ouch. Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis

securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus