The Monthly Security Awareness Newsletter for Everyone

OUCH!

IN THIS ISSUE...

- What Is Encryption?
- What Can You Encrypt?
- Getting It Right

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, encryption can be confusing and you should understand its limitations. In this newsletter, we explain in simple terms what encryption is, how it protects you, and how to implement it properly.

Guest Editor

Francesca Bosco (@francibosco) is a researcher and a project officer, managing projects related to cybercrime, cybersecurity, and the misuse of technology. She is working at the United Nations Interregional Crime and Justice Research Institute and she co-founded the Tech and Law Center.

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

Encryption has been around for thousands of years. Today, encryption is far more sophisticated, but it serves the same purpose -- to pass a secret message from one place to another by ensuring only those authorized to read the message can access it. 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. Today’s 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. In most cases, your key is a password or passcode.

What Can You Encrypt?

In general, there are two types of data to encrypt: data at rest (such as the data stored on your mobile device) and data in motion (such as retrieving email or messaging a friend).

Encryption

Encrypting data at rest is vital to protect information in case your computer or mobile device is lost or stolen. Today's devices are extremely powerful and hold a tremendous amount of information, but are also very easy to lose. In addition, other types of mobile media can hold sensitive information, such as USB flash drives or external hard drives. Full Disk Encryption (FDE) is a widely used encryption technique that encrypts the entire drive in your system. This means that everything on the system is automatically encrypted for you; you do not have to decide what or what not to encrypt. Today, most computers come with FDE, but you may have to manually turn it on or enable it. It is called FileVault on Mac computers, while on Windows computers, depending on the version you have, you can use Bitlocker or Device Encryption. Most mobile devices also support FDE. iOS on iPhones and iPads automatically enable FDE once a passcode has been set. Starting with Android 6.0 (Marshmallow), Google is requiring FDE be enabled by default, provided the hardware meets certain minimum standards.

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

Information is also vulnerable when it is in transit. If the data is not encrypted, it can be monitored, modified, and captured online. This is why you want to ensure that any sensitive online transactions and communications are encrypted. A 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 icon on your browser, or your URL bar turning green. Another example is when you send or receive email. Most email clients provide encrypted capabilities, which you may have to enable. A third example of encrypting data in transit is between two users chatting with each other, such as with iMessage, Wickr, Signal, WhatsApp, or Telegram. Apps like these use end-to-end encryption, which prevents third parties from accessing data while it's transferred from one end system or device to another. This means only you and the person you're communicating with can read what is sent.

Encryption

Getting It Right

To be sure you are protected when using encryption, it is paramount that you use it correctly:

- Your encryption is only as strong as your key. If someone guesses or gets access to your key, they will have access to your data. Protect your key. If you are using a passcode or password for your key, make sure it is a strong, unique password. The longer your password, the harder it is for an attacker to guess or brute force it. Do not forget your password; without your key, you can no longer decrypt your information. If you can't remember all of your passwords, we recommend a password manager.
- Your encryption is only as strong as the security of your devices. If your device has been compromised or is infected by malware, cyber attackers can bypass your encryption. This is why it is so important you take other steps to secure your device, including using anti-virus, strong passwords, and keeping it updated.
- Many mobile apps and computer applications now offer strong encryption to protect your data and communications. If the app or application you are considering does not support encryption, consider an alternative.

Security Awareness Posters

Learn how to protect your family, friends, and coworkers with this series of friendly and free security awareness posters. Download the posters from https://securingthehuman.sans.org/u/i58

Resources

Encryption Explained:	http://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/
Passphrases:	https://securingthehuman.sans.org/ouch/2015#april2015
Password Managers:	https://securingthehuman.sans.org/ouch/2015#october2015
What Is Malware:	https://securingthehuman.sans.org/ouch/2016#march2016
Securing Your New Tablet:	https://securingthehuman.sans.org/ouch/2016#january2016

License