CYBER SECURITY

WHY DOES IT MATTER FOR US

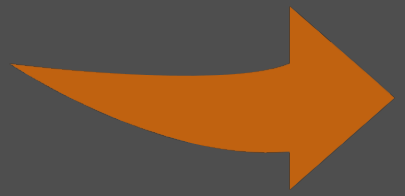
PERCHÈ CI RIGUARDA

CONTENTS



- Cyber attack
- Attackers
- Victims
- Defense
- Women vs Technology
- Q&A

CYBER SECURITY



2017

Rapporto CLUSIT 2018
Sulla sicurezza ICT in Italia

"l'anno del trionfo del Malware, degli attacchi industrializzati realizzati su scala planetaria contro bersagli multipli e della definitiva discesa in campo degli Stati come attori di minaccia".



Rapporto 2018 del Clusit,
Repubblica 28 Febbraion 2018

- Cyber crime affected 1Bn people in the world in 2017
- 500 mld damage
- 1.120 serious attacks in 2017
- Cyber attacks increased of 240% since 2011
- +7% in 2017

Data breach hits Department of Social Services credit card system

Exclusive: Data includes employees' names, user names, work phone numbers, work emails and system passwords

The Gardian UK news 27 November 2017
https://www.theguardian.com/technology/2017/nov/24/data-breach-hits-department-of-social-services-credit-card-system

Attacco alla scuola,

Anonymous vìola i dati di 26 mila prof italiani
26.600 dati personali (email, password, cellulari, indirizzi) di maestre, insegnanti, referenti e dirigenti di molte scuole italiane

La Repubblica 08 Marzo 2018 http://www.repubblica.it/tecnologia/sicurezza/2018/03/08/news/attacco_alla_scuola_anonymous_viola_i_dati_di_26_mila_prof_italiani-190799922/

CYBER ATTACK

- Phishing
- Ransomware
- Impersonation attacks
- Credential stealer
- Malware
- Crypto stealer

- Financial loss
- Fraud
- Identity theft
- Data confidentiality and integrity breach
- Reputational damage
- Computing power stolen by hackers

TYPE OF CYBER ATTACKS

- Phishing
- Malware
- Ransomware attacks
- Web attacks
- Email and account attacks

RESULTS

- Data exfiltration
- Digital fraud (i.e.credit cards, home banking)
- Data encrypted asking ransom in crypto currencies
- Web sites unavailable
- SPAM attack from compromised accounts
- Impersonating others to make fraud online
- Computing power stealer

ATTACKERS

	Motivation	Objective
Hackers	Financial gain	Money
Hacktivist	Political, religious	Sabotage
State-sponsored	Political influence, market competitive advantage	Espionage

VICTIMS

	Preferred attack vector	Goal
People	Phishing and social media	Money, fraud, damage reputation
Children and young girls and boys	Social media	Pornography, pedo-pornograpy, cyber bullying, trafficking
Small business	Phishing Malware	Fraud, damage reputation
Corporate	Phishing, Spear phishing, Malware, Identity theft	Fraud, damage reputation, competitive advantage
Government, Institutions	Phishing, Spear phishing, Malware, fake news	Espionage, damage reputation, political influence

DIGITAL TRASFORMATION

DISRUPTIVE TECHNOLOGY

- Letters vs emails
- Phone vs Smartphone
- Photo vs Digital image
- Phone call vs Skype call
- Watch TV program vs Video streaming (YouTube, NetFlix)
- Desk vs Laptop
- Tour operator vs online Booking
- Bank branch vs Home banking
- Meet people vs Social media

DEFENCE

- Backup your data
- Patch your system (Windows update, Security update)
- Antivirus and Antimalware or Windows Defender
- Use a good password (at least 8 alpanumerical characters and special characters)
- NEVER disclouse your password
- Pay attention to phishing
- Do not give away personal information

THANK YOU FOR YOUR ATTENTION

For any question,
contact me at
l.bia@outlook.com



Laura Biagiotti
CISM CRISC

National Cyber Security Centre
a part of GCHQ

Cyber Security
Small Charity Guide

This advice has been produced to help charities protect themselves from the most common cyber attacks. The 5 topics covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at **www.ncsc.gov.uk/charity** .

Backing up your data

Take *regular* backups of your important data, and *test* they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.

- **Identify what needs to be backed up.** Normally this will comprise documents, emails, contacts, legal information, calendars, financial records and supporter or beneficiary databases.
- **Ensure the device containing your backup is *not* permanently connected** to the device holding the original copy, neither physically nor over a local network.
- **Consider backing up to the cloud.** This means your data is stored in a separate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.

Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than 'desktop' equipment.

- **Switch on PIN/password protection/fingerprint recognition** for mobile devices.
- Configure devices so that when lost or stolen they can be **tracked**, **remotely wiped** or **remotely locked**.
- Keep your **devices** (and all **installed apps**) **up to date**, using the '**automatically update**' option if available.
- When sending sensitive data, don't connect to public Wi-Fi hotspots - **use 3G or 4G connections** (including tethering and wireless dongles) or **use VPNs**.
- **Replace devices that are no longer supported by manufacturers** with up-to-date alternatives.

Preventing malware damage

You can protect your charity from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.

- **Use antivirus** software on all computers and laptops. **Only install approved software** on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.
- **Patch all software and firmware** by promptly applying the latest software updates provided by manufacturers and vendors. Use the '**automatically update**' option where available.
- **Control access to removable media** such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.
- **Switch on your firewall** (included with most operating systems) to create a buffer zone between your network and the Internet.

Avoiding phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.

- Ensure staff **don't browse the web or check emails** from an account with **Administrator privileges**. This will reduce the impact of successful phishing attacks.
- **Scan for malware** and **change passwords** as soon as possible if you suspect a successful attack has occurred. **Don't punish staff** if they get caught out (it discourages people from reporting in the future).
- Check for obvious signs of phishing, like **poor spelling and grammar**, or **low quality versions** of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

Using passwords to protect your data

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.



- Make sure all laptops, MACs and PCs **use encryption products** that require a password to boot. Switch on **password/PIN protection** or **fingerprint recognition** for mobile devices.
- **Use two factor authentication (2FA)** for important websites like banking and email, if you're given the option.
- **Avoid using predictable passwords** (such as family and pet names). Avoid the most common passwords that criminals can guess (like *passw0rd*).
- Do not enforce regular password changes; they only need to be changed when you suspect a compromise.
- **Change** the manufacturers' default passwords that devices are issued with, before they are distributed to staff.
- **Provide secure storage** so staff can write down passwords and keep them safe (but not with the device). Ensure staff can reset their own passwords, easily.
- **Consider using a password manager.** If you do use one, make sure that the 'master' password (that provides access to all your other passwords) is a strong one.



© Crown Copyright 2018