13/02/2020

THURSDAY THOUGHTS

Business to Business Marketing

The ICO shared their guidance on business to business marketing. Starting with the age-old question "Does GDPR apply to business-to-business marketing?" – the answer is (of course) Yes! GDPR applies whenever personal data is processed and in the business context that includes where you keep the name and number of a business contact on file, including if you file loose business cards. What many are unaware of is that personal information also includes a business email address that contains a person's name. Here is a summary of the guidance:

- GDPR **does not** replace PECR.
- You do not always require consent for marketing under GDPR (but you may need consent to comply with the PECR).
- You can rely on legitimate interests for marketing activities if:
    - you don't need consent under PECR.
    - you can demonstrate your use is proportionate
    - if your marketing has minimal privacy impact
    - people would not be surprised or likely to object to what you are doing
- A new ePrivacy Regulation is expected in the near future.
- Sole traders and some partnerships are treated as individuals so be careful sending marketing emails or texts.
- You must include an opt-out or unsubscribe option in the message.
- You can email or text any corporate body using a generic email address (e.g. "info@", "hello@") but it is good practice to keep a "do not contact" list.

You can read the full ICO guidance here http://ow.ly/jUbP50xxdfg

Draft Direct Marketing Code of Practice

The ICO has launched a public consultation on their draft direct marketing code of practice. The consultation ends on 4 March 2020

with the “final” document due later in 2020. If you wish to take part it is on their website.
https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-on-the-draft-direct-marketing-code-of-practice/

Altrincham Chamber of Commerce GDPR Clinic

PPPManagement ran a very successful GDPR Clinic with Slater Heelis at the February Altrincham Chamber of Commerce Breakfast. Providing real life examples, practical hints and no scaremongering. We also introduced our GDPR Snakes and Ladders Game (trade mark pending) which proved to be very popular.

Hanna Andersson/Salesforce Breach

A class action lawsuit has been taken out against Hanna Andersson and Salesforce.com following a data breach which affected an estimated 10,000 customers. Unencrypted personal information (including name, shipping address, billing address, payment card number, CVV code, and expiration date) was made available to hackers when malware attacked Hanna’s e-commerce platform between September and Nov 2019. The companies only became aware of it when law enforcement found customers’ stolen information on the dark web.

This makes troubling reading for UK businesses using Salesforce. To date the organisation hasn’t notified the authorities in California that they have suffered a breach. Certainly something to look into if you use a cloud provider as your processor. At the very least check that their responsibilities in the event of a breach are what you expect them to be!

Facebook Twitter Account

The recent hack of Facebook’s Twitter account shows even the tech giants can fall victim to such attacks. Many businesses use third-party software as a convenient way to manage their social media. Davey Winder in an article in Forbes recommends that if you use third party software you should consider “revoking all third-party platform access which doesn’t offer robust multi-factor authenticator app protection”. Apparently the route into the third-party platform was by resetting passwords and email addresses. You can read the detail here https://www-forbes-com.cdn.ampproject.org/c/s/www.forbes.com/sites/daveywinder/2020/02/08/facebook-hack-social-network-confirms-134-million-follower-twitter-account-compromised/amp/

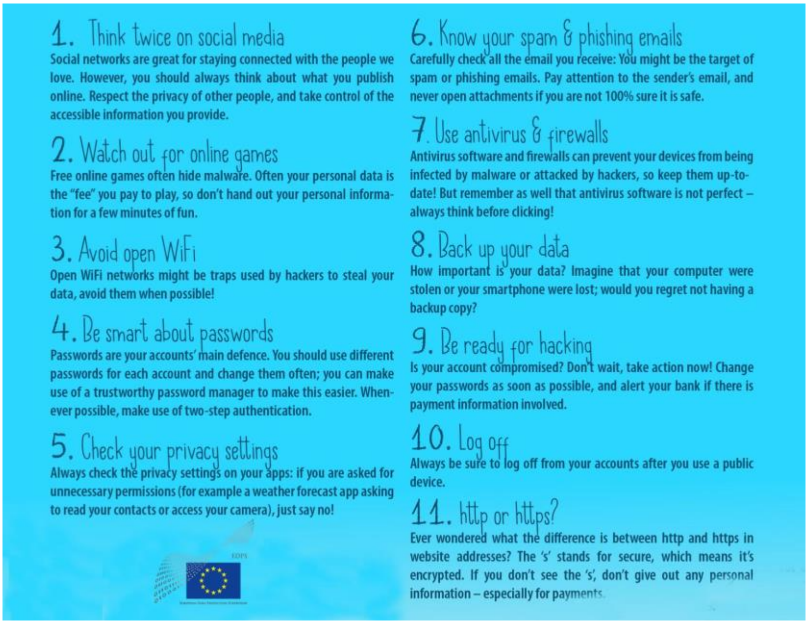
Shopping Online Securely

The UK National Cyber Security Centre published guidance on shopping on line securely. Reminding users that they don’t have to share all their details with a business just because they ask for it. Top tips from their article:

- Checkout as a guest
- Look for a padlock in the address bar
- Only fill in the mandatory details of forms
- Only create an account on a new site if you’re going to it a lot in the future.
- Don't give away too much information
- Keep your devices up to date
- Use a strong password
- Turn on two-factor authentication (2FA)

Safer Internet Day

The 11th February was The European Data Protection Supervisor shared a useful infographic with 11 hints



1. Think twice on social media

Social networks are great for staying connected with the people we love. However, you should always think about what you publish online. Respect the privacy of other people, and take control of the accessible information you provide.

2. Watch out for online games

Free online games often hide malware. Often your personal data is the "fee" you pay to play, so don't hand out your personal information for a few minutes of fun.

3. Avoid open WiFi

Open WiFi networks might be traps used by hackers to steal your data, avoid them when possible!

4. Be smart about passwords

Passwords are your accounts' main defence. You should use different passwords for each account and change them often; you can make use of a trustworthy password manager to make this easier. Whenever possible, make use of two-step authentication.

5. Check your privacy settings

Always check the privacy settings on your apps: if you are asked for unnecessary permissions (for example a weather forecast app asking to read your contacts or access your camera), just say no!

6. Know your spam & phishing emails

Carefully check all the email you receive: You might be the target of spam or phishing emails. Pay attention to the sender's email, and never open attachments if you are not 100% sure it is safe.

7. Use antivirus & firewalls

Antivirus software and firewalls can prevent your devices from being infected by malware or attacked by hackers, so keep them up-to-date! But remember as well that antivirus software is not perfect – always think before clicking!

8. Back up your data

How important is your data? Imagine that your computer were stolen or your smartphone were lost; would you regret not having a backup copy?

9. Be ready for hacking

Is your account compromised? Don't wait, take action now! Change your passwords as soon as possible, and alert your bank if there is payment information involved.

10. Log off

Always be sure to log off from your accounts after you use a public device.

11. http or https?

Ever wondered what the difference is between http and https in website addresses? The 's' stands for secure, which means it's encrypted. If you don't see the 's', don't give out any personal information – especially for payments.

Use of Third-Party Email Apps

In an article for iDrop News, Jesse Hollington cites a Motherboard report that found that many of third-party email apps scrape data from users' inboxes and sell it to advertising and marketing companies. The problem is with third-party iOS apps that offer immediate push notifications for new messages. Apps such as Edison, Cleanfox and Rakuten's Slice provide users with the opportunity to opt out of the data scraping but many users are unaware that the data is being gathered in the first place!

Estee Lauder Data Breach

An unsecured database belonging to cosmetic giant Estee Lauder exposed hundreds of millions of customer records and internal logs. At the end of January 2020 it was discovered Estee Lauder's shared database was unsecured - 440,336,852 records, including information in plain text such as email addresses, production, audit and middleware logs were available for all to read. The lesson to us all is to make sure we secure all our databases so that unauthorised users cannot get access!

The Need for Clarity in Breach Disclosure Letters

Breach information should be as clear and precise as possible. An example of a “vague and deceptive” breach disclosure letter came from an American bank. Fifth Third wrote to an undisclosed number of clients to tell them that a “small number of employees” had stolen customer information and given it to a third party. It was not just the client accounts that were compromised as the stolen information included names, Social Security numbers, addresses, dates of birth, phone numbers, mothers’ maiden names, driver’s license information, and account numbers. In its disclosure letter the bank said the theft was uncovered following an internal investigation but that it could not provide detail because of an active investigation boing on to say “Incidents like this are rare, nonetheless, we are reviewing our current preventative measures to determine how we might further increase their effectiveness.”

Facial Recognition Technology Deployed in Stratford

The Met used facial recognition technology in Stratford for the first time on 11 February. They chose this area because the local community supports the police in using any tactic to deal with violence. Cameras on a dark blue van scanned and cross-matched every passing face against a watch list of 5,000 profiles. Looking for people wanted for serious criminal offences or by the courts or for investigation. There were signs surrounding the van to say the technology was in use and that people were not required to pass through the system. It will be interesting to see what the information commissioner, the surveillance camera commissioner and the biometric commissioner have to say on the matter.

Facebook Dating Service Postponed

Facebook suspended the roll out of its dating service in Europe planned the eve of Valentine's Day after officials from the Irish data

regulator searched its offices. The regulator was concerned that it had only just heard about the feature and added that the company had not provided it with a data protection assessment of the dating service.
You must do a DPIA if your processing is likely to result in a high risk to individuals. But it is good practice to do a DPIA for any other major project which requires the processing of personal data.

PayPal Phishing email.

Beware of any email that asks you to verify your identity by clicking on the button “Secure and update my account now!”. It is, sadly, likely to be fraudulent. In this recent example when you click the button, you are redirected to a page which looks like the genuine PayPal login screen but once you log in more personal data is asked for including a copy of your ID, Social Security number or passport, in order to authenticate your identity. There is no confirmation after any uploads, thus victims may end up uploading more documents thinking that previous attempts were invalid. This latest PayPal phishing email has “Support” as part of the email address.

If in doubt log in to PayPal on their secure website - don't take risks with your personal data!