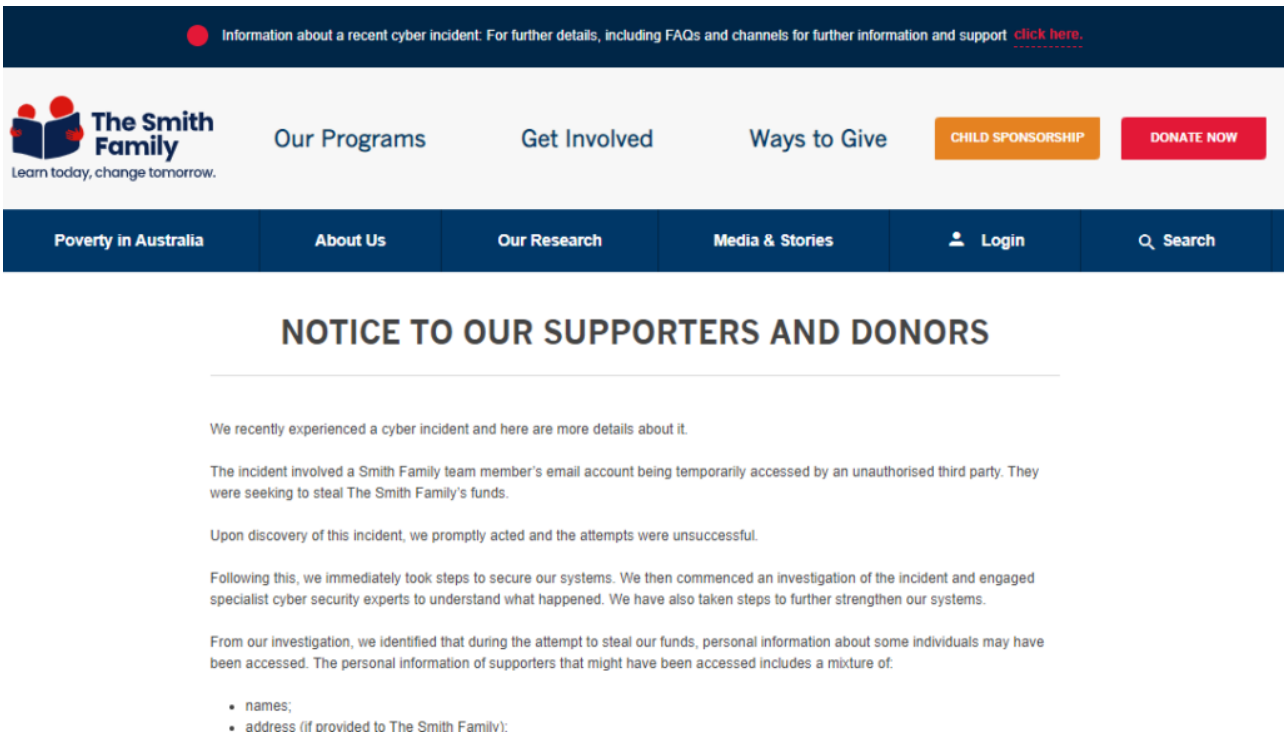
Comment réagir à un piratage de données – l’exemple de Smith Family

L’association australienne Smith Family (collecte annuelle environ 80M€) a été récemment victime d’une cyber attaque. Parallèlement aux actions techniques, sa réaction en termes de communication a consisté en la mise en avant sur son site d’une page dédiée explicative sur les circonstances de l’incident et ses conséquences pour les personnes concernées.



Une communication la plus transparente possible, organisée en 3 volets

Informer

NOTICE TO OUR SUPPORTERS AND DONORS

We recently experienced a cyber incident and here are more details about it.

The incident involved a Smith Family team member's email account being temporarily accessed by an unauthorised third party. They were seeking to steal The Smith Family's funds.

Upon discovery of this incident, we promptly acted and the attempts were unsuccessful.

Following this, we immediately took steps to secure our systems. We then commenced an investigation of the incident and engaged specialist cyber security experts to understand what happened. We have also taken steps to further strengthen our systems.

From our investigation, we identified that during the attempt to steal our funds, personal information about some individuals may have been accessed. The personal information of supporters that might have been accessed includes a mixture of:

- names;
- address (if provided to The Smith Family);
- phone number (if provided to The Smith Family);
- email address (if provided to The Smith Family); and
- donation amount.

And in some cases:

- first 4 and last 4 digits of the credit or debit card used to donate; and,
- information about whether a donation payment was processed successfully or declined

We can confirm for those with potential credit or debit card details accessed, no middle digits, or CVV numbers were accessed as The Smith Family does not store that information in its systems.

The data accessed in itself cannot be used to make fraudulent purchases.

Our investigation also identified some other information which may have been accessed but does not require formal notification.

The Smith Family also does not request, collect or hold personal identity documents such as passports or drivers' licences of our supporters, as these are not required to process their generous donations.

While there is no current evidence of misuse of any individual's personal information, we are informing individuals about the incident and providing simple steps to protect their information and avoid any potential scams.

We are also contacting individuals whose personal information was not accessed and are not directly affected by this incident as we want to communicate transparently to our supporters.

- Cet incident a-t-il un rapport avec le vol de données Medibank ?
- Les autorités ont-elles été informées ?
- Comment puis-je savoir que cette affaire sera terminée pour ce qui me concerne ?

Expliquer

- Comment nous-sommes-nous rendu compte de l’incident
- Comment le pirate a-t-il pu accéder à l’email de notre collaborateur
- Pourquoi Smith Family dispose-t-elle d’informations personnelles à mon sujet ?

Rassurer

- L’attaque a-t-elle été interrompue

- Des données personnelles ont-elles été divulguées
- Comment savez-vous qu’aucune donnée personnelle n’a été utilisée
- Nos systèmes sont-ils toujours opérationnels ?
- Dois-je annuler ma carte bancaire ?
- Que dois-je faire maintenant ?
- Puis-je toujours faire un don en ligne ?

Pour information, l’association semble utiliser la solution CRM Dynamics 365. *voir ici*