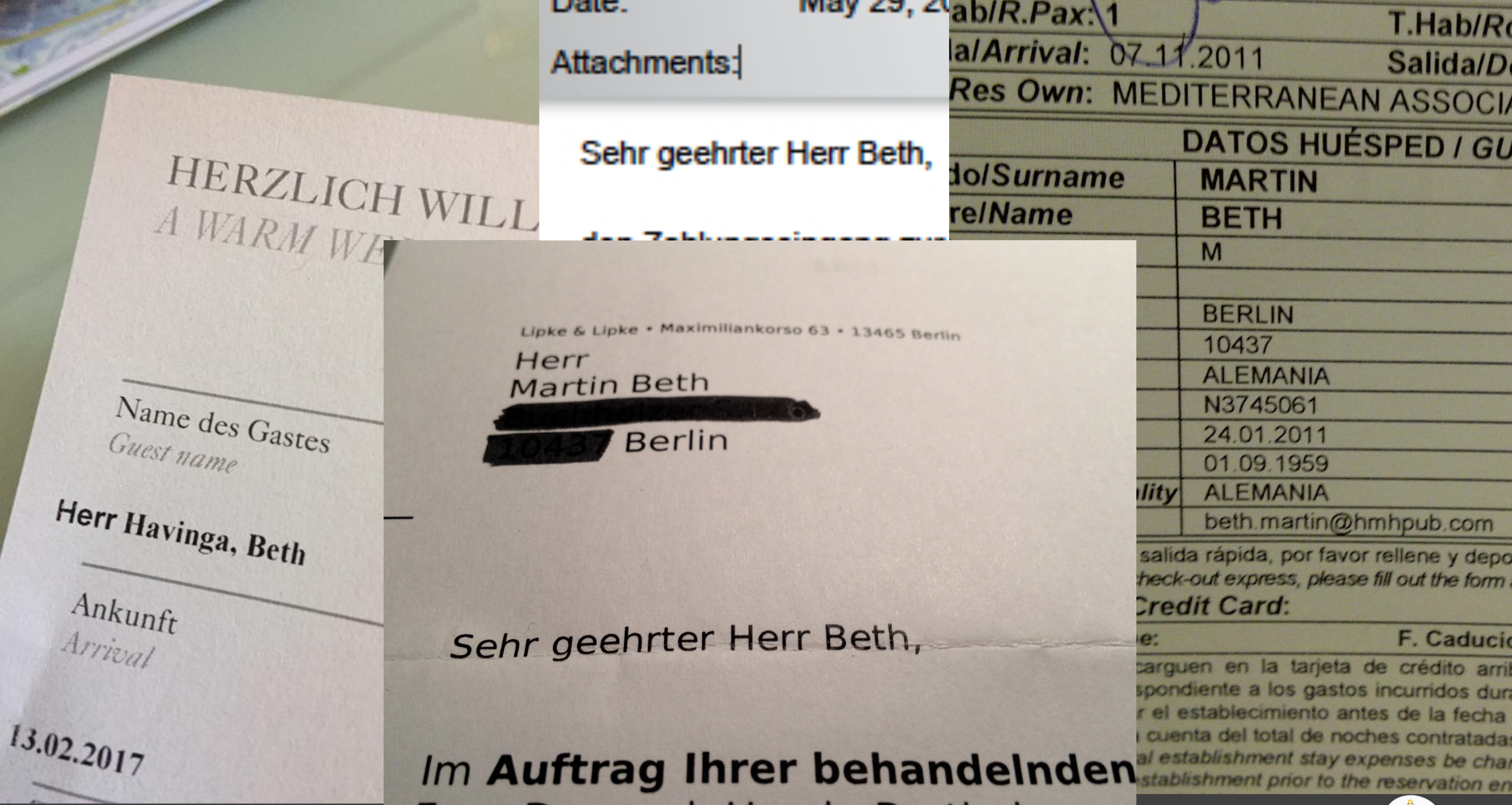
IDM als Schlüssel in der Bildung?

Beth Havinga
16 Februar 2023

www.connect-edtech.com

Wieso sind digitale Identitäten so wichtig?



HERZLICH WILL

A WARM WE

Name des Gastes
Guest name

Herr Havinga, Beth

Ankunft
Arrival

13.02.2017

Date: May 29, 2

Attachments:

Sehr geehrter Herr Beth,

Lipke & Lipke • Maximiliankorso 63 • 13465 Berlin

Herr
Martin Beth
[redacted]
[redacted] Berlin

Sehr geehrter Herr Beth,

Im **Auftrag Ihrer behandelnden**

ab/R.Pax: 1 T.Hab/R

a/Arrival: 07.11.2011 Salida/D

Res Own: MEDITERRANEAN ASSOCI

DATOS HUÉSPED / GU

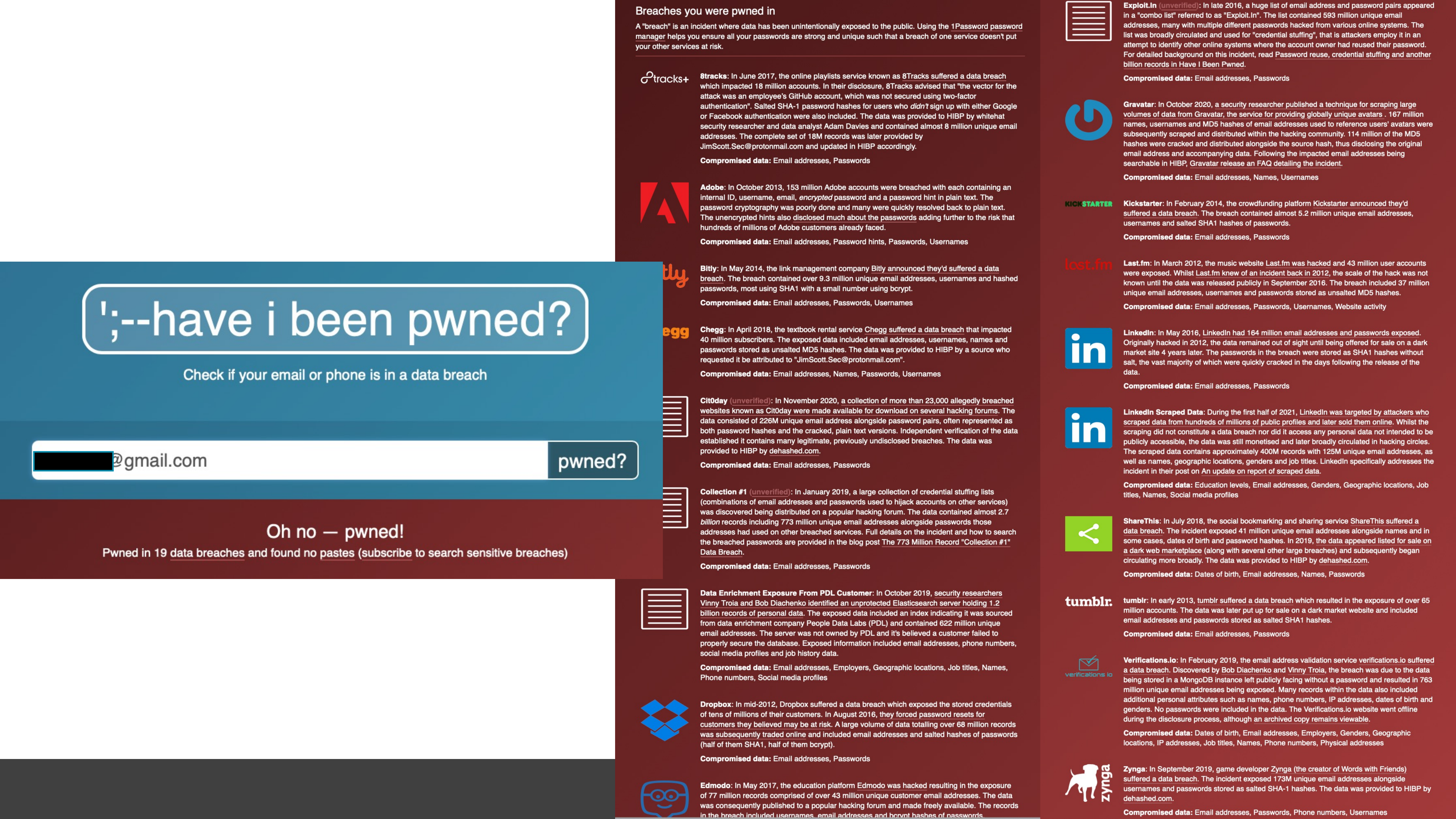
do/Surname	MARTIN
re/Name	BETH
	M
	BERLIN
	10437
	ALEMANIA
	N3745061
	24.01.2011
	01.09.1959
lity	ALEMANIA
	beth.martin@hmhpub.com

salida rápida, por favor rellene y depo
heck-out express, please fill out the form

Credit Card:

e: F. Caduci

carguen en la tarjeta de crédito arr
spondiente a los gastos incurridos dur
r el establecimiento antes de la fecha
cuenta del total de noches contratada
al establishment stay expenses be cha
stablishment prior to the reservation en



Check if your email or phone is in a data breach

[redacted]@gmail.com

Oh no — pwned!

Pwned in 19 data breaches and found no pastes (subscribe to search sensitive breaches)

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

8tracks: In June 2017, the online playlists service known as 8Tracks suffered a data breach which impacted 18 million accounts. In their disclosure, 8Tracks advised that "the vector for the attack was an employee's GitHub account, which was not secured using two-factor authentication". Salted SHA-1 password hashes for users who *didn't* sign up with either Google or Facebook authentication were also included. The data was provided to HIBP by whitehat security researcher and data analyst Adam Davies and contained almost 8 million unique email addresses. The complete set of 18M records was later provided by JimScott.Sec@protonmail.com and updated in HIBP accordingly.

Compromised data: Email addresses, Passwords

Adobe: In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

Compromised data: Email addresses, Password hints, Passwords, Usernames

Bitly: In May 2014, the link management company Bitly announced they'd suffered a data breach. The breach contained over 9.3 million unique email addresses, usernames and hashed passwords, most using SHA1 with a small number using bcrypt.

Compromised data: Email addresses, Passwords, Usernames

Chegg: In April 2018, the textbook rental service Chegg suffered a data breach that impacted 40 million subscribers. The exposed data included email addresses, usernames, names and passwords stored as unsalted MD5 hashes. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Compromised data: Email addresses, Names, Passwords, Usernames

Cit0day (unverified): In November 2020, a collection of more than 23,000 allegedly breached websites known as Cit0day were made available for download on several hacking forums. The data consisted of 226M unique email address alongside password pairs, often represented as both password hashes and the cracked, plain text versions. Independent verification of the data established it contains many legitimate, previously undisclosed breaches. The data was provided to HIBP by dehashed.com.

Compromised data: Email addresses, Passwords

Collection #1 (unverified): In January 2019, a large collection of credential stuffing lists (combinations of email addresses and passwords used to hijack accounts on other services) was discovered being distributed on a popular hacking forum. The data contained almost 2.7 *billion* records including 773 million unique email addresses alongside passwords those addresses had used on other breached services. Full details on the incident and how to search the breached passwords are provided in the blog post The 773 Million Record "Collection #1" Data Breach.

Compromised data: Email addresses, Passwords

Data Enrichment Exposure From PDL Customer: In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.

Compromised data: Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Social media profiles

Dropbox: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

Compromised data: Email addresses, Passwords

Edmodo: In May 2017, the education platform Edmodo was hacked resulting in the exposure of 77 million records comprised of over 43 million unique customer email addresses. The data was consequently published to a popular hacking forum and made freely available. The records in the breach included usernames, email addresses and bcrypt hashes of passwords

Exploit.In (unverified): In late 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Exploit.In". The list contained 593 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read Password reuse, credential stuffing and another billion records in Have I Been Pwned.

Compromised data: Email addresses, Passwords

Gravatar: In October 2020, a security researcher published a technique for scraping large volumes of data from Gravatar, the service for providing globally unique avatars . 167 million names, usernames and MD5 hashes of email addresses used to reference users' avatars were subsequently scraped and distributed within the hacking community. 114 million of the MD5 hashes were cracked and distributed alongside the source hash, thus disclosing the original email address and accompanying data. Following the impacted email addresses being searchable in HIBP, Gravatar release an FAQ detailing the incident.

Compromised data: Email addresses, Names, Usernames

Kickstarter: In February 2014, the crowdfunding platform Kickstarter announced they'd suffered a data breach. The breach contained almost 5.2 million unique email addresses, usernames and salted SHA1 hashes of passwords.

Compromised data: Email addresses, Passwords

Last.fm: In March 2012, the music website Last.fm was hacked and 43 million user accounts were exposed. Whilst Last.fm knew of an incident back in 2012, the scale of the hack was not known until the data was released publicly in September 2016. The breach included 37 million unique email addresses, usernames and passwords stored as unsalted MD5 hashes.

Compromised data: Email addresses, Passwords, Usernames, Website activity

LinkedIn: In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

Compromised data: Email addresses, Passwords

LinkedIn Scraped Data: During the first half of 2021, LinkedIn was targeted by attackers who scraped data from hundreds of millions of public profiles and later sold them online. Whilst the scraping did not constitute a data breach nor did it access any personal data not intended to be publicly accessible, the data was still monetised and later broadly circulated in hacking circles. The scraped data contains approximately 400M records with 125M unique email addresses, as well as names, geographic locations, genders and job titles. LinkedIn specifically addresses the incident in their post on An update on report of scraped data.

Compromised data: Education levels, Email addresses, Genders, Geographic locations, Job titles, Names, Social media profiles

ShareThis: In July 2018, the social bookmarking and sharing service ShareThis suffered a data breach. The incident exposed 41 million unique email addresses alongside names and in some cases, dates of birth and password hashes. In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by dehashed.com.

Compromised data: Dates of birth, Email addresses, Names, Passwords

tumblr: In early 2013, tumblr suffered a data breach which resulted in the exposure of over 65 million accounts. The data was later put up for sale on a dark market website and included email addresses and passwords stored as salted SHA1 hashes.

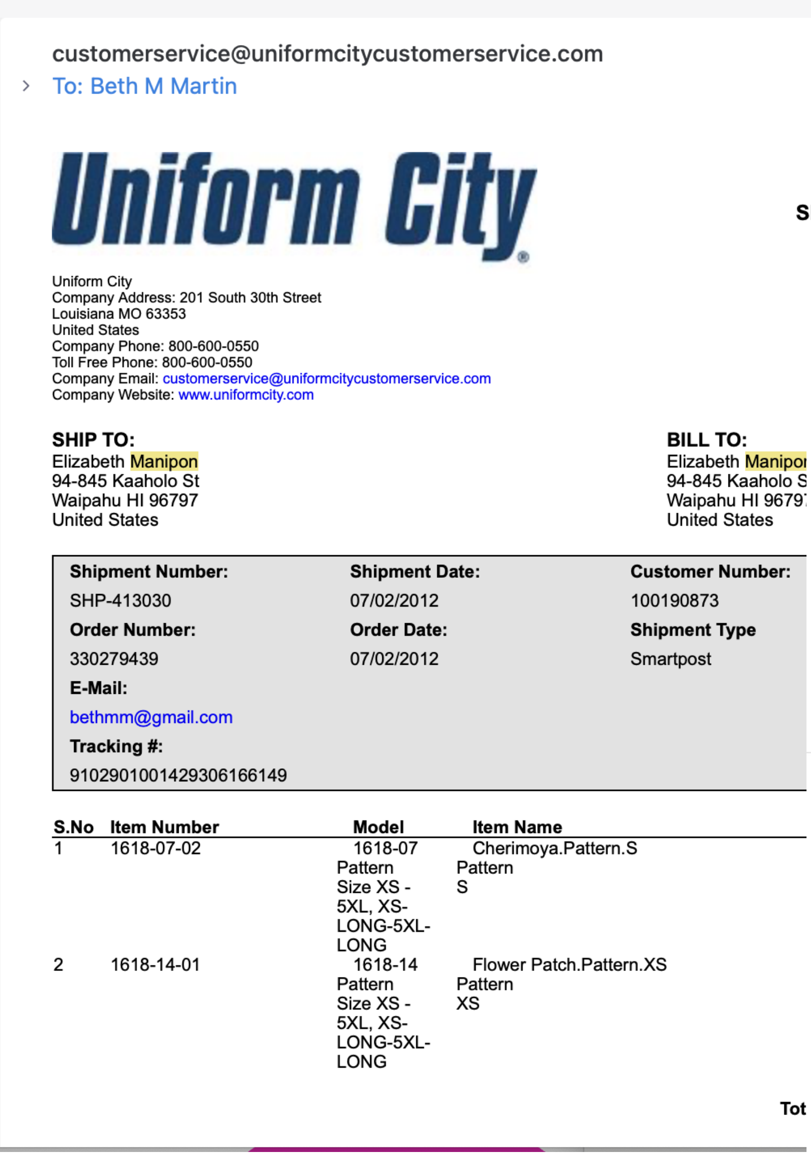
Compromised data: Email addresses, Passwords

Verifications.io: In February 2019, the email address validation service verifications.io suffered a data breach. Discovered by Bob Diachenko and Vinny Troia, the breach was due to the data being stored in a MongoDB instance left publicly facing without a password and resulted in 763 million unique email addresses being exposed. Many records within the data also included additional personal attributes such as names, phone numbers, IP addresses, dates of birth and genders. No passwords were included in the data. The Verifications.io website went offline during the disclosure process, although an archived copy remains viewable.

Compromised data: Dates of birth, Email addresses, Employers, Genders, Geographic locations, IP addresses, Job titles, Names, Phone numbers, Physical addresses

Zynga: In September 2019, game developer Zynga (the creator of Words with Friends) suffered a data breach. The incident exposed 173M unique email addresses alongside usernames and passwords stored as salted SHA-1 hashes. The data was provided to HIBP by dehashed.com.

Compromised data: Email addresses, Passwords, Phone numbers, Usernames



customerservice@uniformcitycustomerservice.com

To: Beth M Martin

Uniform City

Uniform City
Company Address: 201 South 30th Street
Louisiana MO 63353
United States
Company Phone: 800-600-0550
Toll Free Phone: 800-600-0550
Company Email: customerservice@uniformcitycustomerservice.com
Company Website: www.uniformcity.com

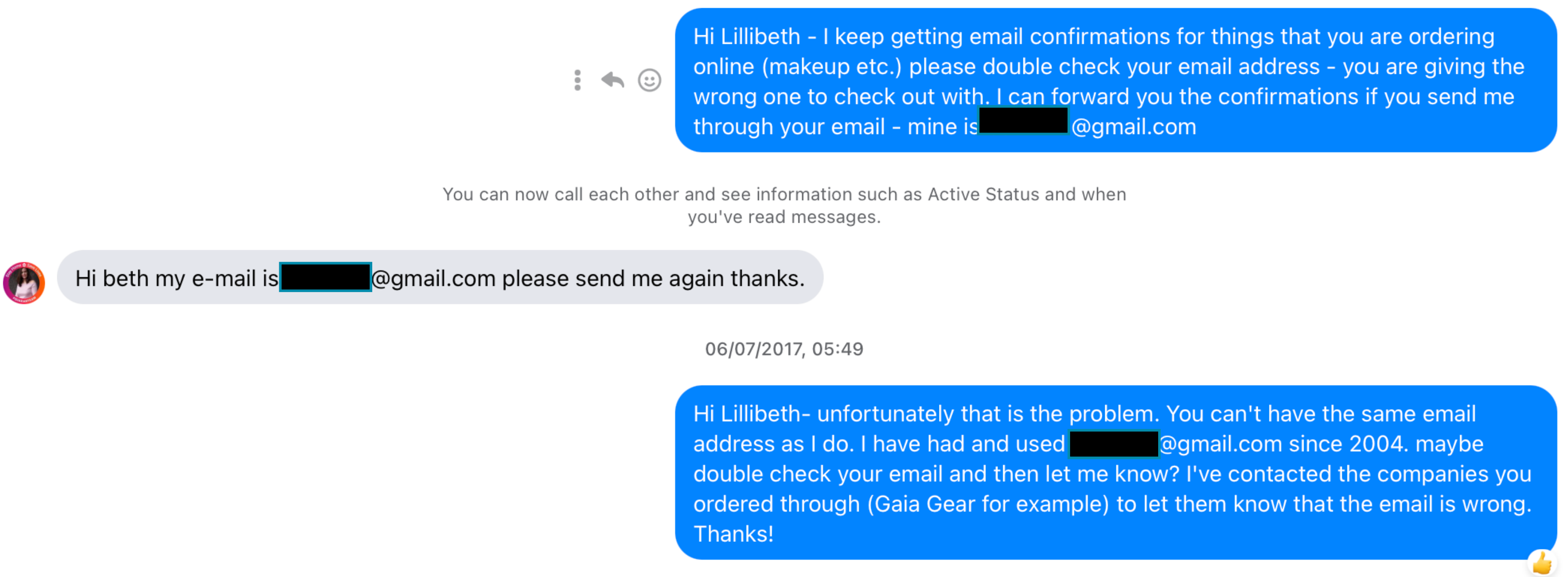
SHIP TO:
Elizabeth Manipon
94-845 Kaaholo St
Waipahu HI 96797
United States

BILL TO:
Elizabeth Manipor
94-845 Kaaholo S
Waipahu HI 9679
United States

Shipment Number:	**Shipment Date:**	**Customer Number:**
SHP-413030	07/02/2012	100190873
Order Number:	**Order Date:**	**Shipment Type**
330279439	07/02/2012	Smartpost
E-Mail:		
bethmm@gmail.com		
Tracking #:		
9102901001429306166149		

S.No	Item Number	Model	Item Name
1	1618-07-02	1618-07 Pattern Size XS - 5XL, XS-LONG-5XL-LONG	Cherimoya.Pattern.S Pattern S
2	1618-14-01	1618-14 Pattern Size XS - 5XL, XS-LONG-5XL-LONG	Flower Patch.Pattern.XS Pattern XS

Tot



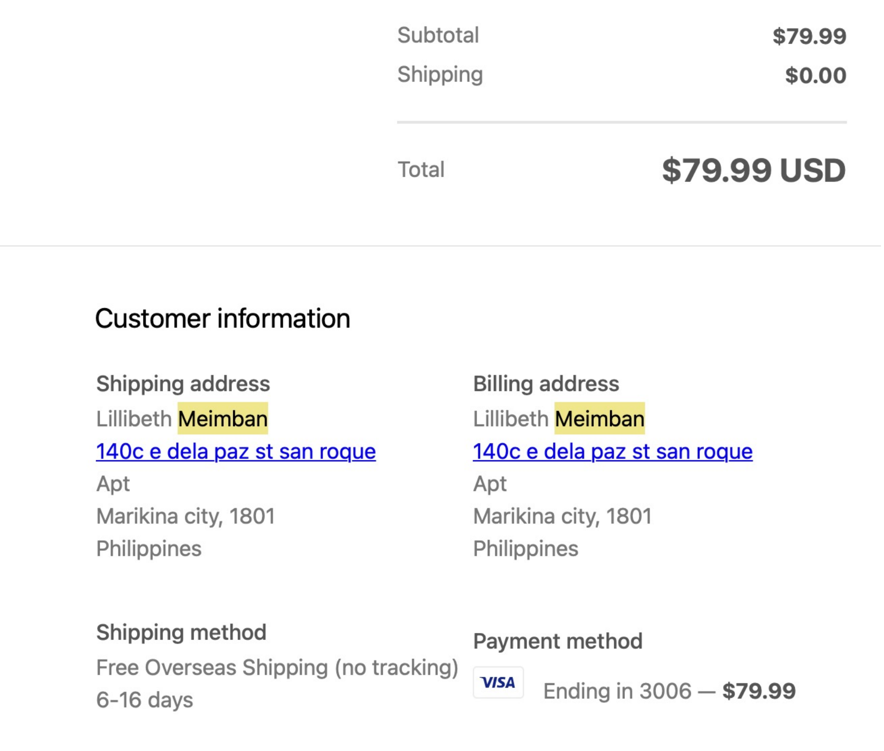
Hi Lillibeth - I keep getting email confirmations for things that you are ordering online (makeup etc.) please double check your email address - you are giving the wrong one to check out with. I can forward you the confirmations if you send me through your email - mine is [redacted]@gmail.com

You can now call each other and see information such as Active Status and when you've read messages.

Hi beth my e-mail is [redacted]@gmail.com please send me again thanks.

06/07/2017, 05:49

Hi Lillibeth- unfortunately that is the problem. You can't have the same email address as I do. I have had and used [redacted]@gmail.com since 2004. maybe double check your email and then let me know? I've contacted the companies you ordered through (Gaia Gear for example) to let them know that the email is wrong. Thanks!



Shipping Con

Or

Subtotal	$79.99
Shipping	$0.00
Total	$79.99 USD

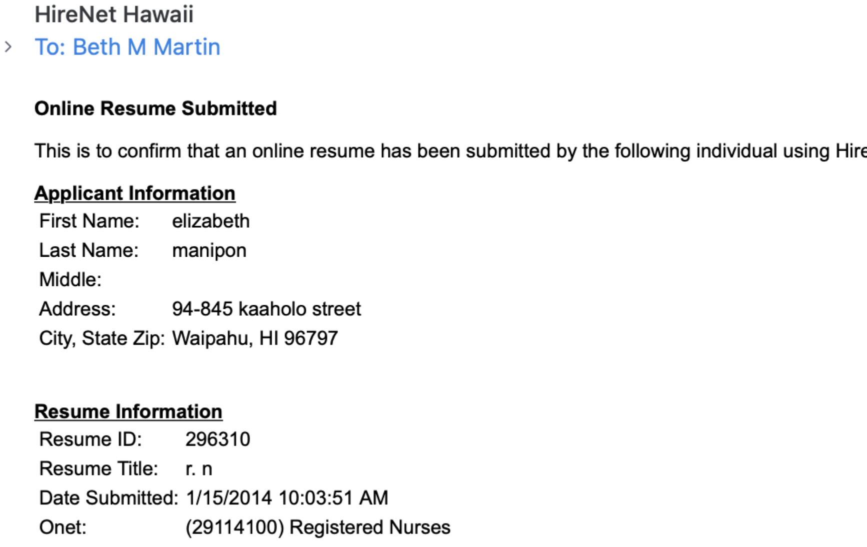
Customer information

Shipping address
Lillibeth Meimban
140c e dela paz st san roque
Apt
Marikina city, 1801
Philippines

Billing address
Lillibeth Meimban
140c e dela paz st san roque
Apt
Marikina city, 1801
Philippines

Shipping method
Free Overseas Shipping (no tracking)
6-16 days

Payment method
VISA Ending in 3006 — **$79.99**



HireNet Hawaii

To: Beth M Martin

Online Resume Submitted

This is to confirm that an online resume has been submitted by the following individual using Hire

Applicant Information

First Name:	elizabeth
Last Name:	manipon
Middle:	
Address:	94-845 kaaholo street
City, State Zip:	Waipahu, HI 96797

Resume Information

Resume ID:	296310
Resume Title:	r. n
Date Submitted:	1/15/2014 10:03:51 AM
Onet:	(29114100) Registered Nurses

Identitäten Fails (mit extremen Nachwirkungen)

- Die Identität ist falsch aber mit Dir verbunden
- Die Identität wurde gehackt
- Andere nutzen die Identität (aus Versehen oder mit Absicht)
- Die Identität ist nicht mehr verbunden

im Jahr 2020/21 haben Lernende im Durchschnitt 143 EdTech Werkzeuge benutzt

https://www.k12dive.com/news/students-used-average-of-143-ed-tech-tools-in-2021-22/630173/

1600

Was ist Identitätsmanagement?

- Wie man sich identifiziert
- Welche Informationen mitgegeben werden
- Zugang mittels der Identität bei mehreren Dienstleistungen bekommen

Identitäten sind mehr als ein Login

- Künstliche Intelligenz
- Systeme, die Lernen (und profitieren) von deinen Aktivitäten
- Wie man aufgefunden werden kann
- Wie man sich verbinden kann

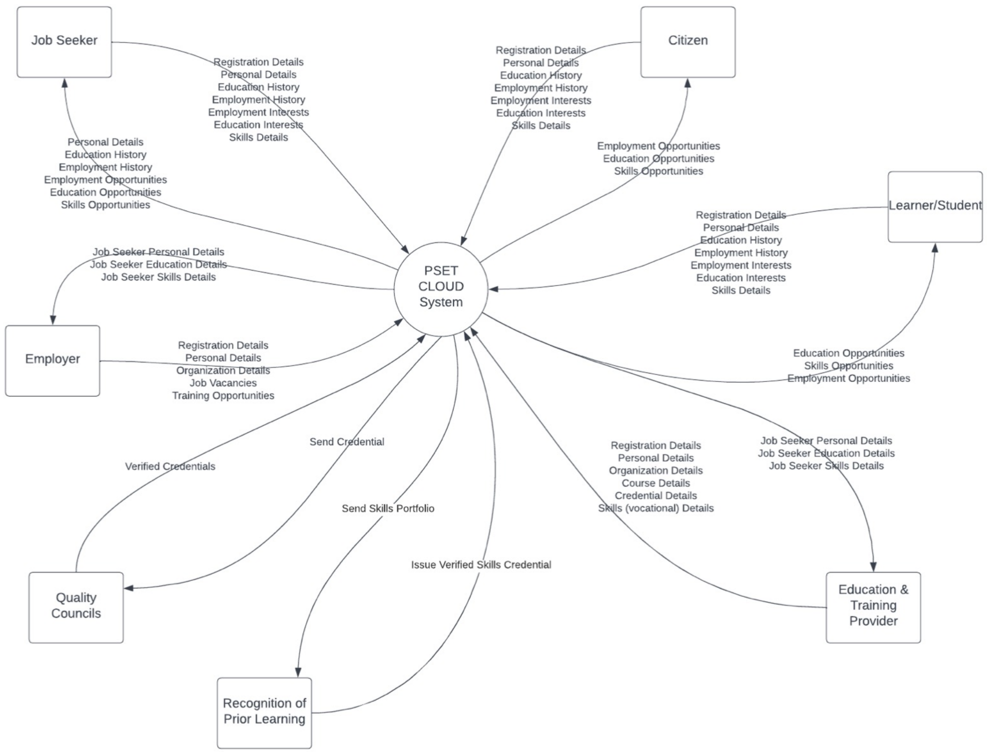
andrea-de-santis-zwd435-ewb4-unsplash

IDM ist nicht nur IDM

- Datenmanagement/ -modelle / -mobilität
- Interoperabilität/ Anschlussfähigkeit
- (Daten)sicherheit und (-)Schutz
- Übergreifende (Standardisierungs)verfahren

Wallets

- Lebenslanges Lernen (und ID)
- Weltweites Thema
- EU: Digitales Portmonnaie
- Verschiedene Umsetzungen - zentrale Datenstores, Eigentumsrechte



Job Seeker

Citizen

Learner/Student

Employer

PSET CLOUD System

Quality Councils

Recognition of Prior Learning

Education & Training Provider

Registration Details
Personal Details
Education History
Employment History
Employment Interests
Education Interests
Skills Details

Personal Details
Education History
Employment History
Employment Opportunities
Education Opportunities
Skills Opportunities

Registration Details
Personal Details
Education History
Employment History
Employment Interests
Education Interests
Skills Details

Employment Opportunities
Education Opportunities
Skills Opportunities

Registration Details
Personal Details
Education History
Employment History
Employment Interests
Education Interests
Skills Details

Job Seeker Personal Details
Job Seeker Education Details
Job Seeker Skills Details

Registration Details
Personal Details
Organization Details
Job Vacancies
Training Opportunities

Education Opportunities
Skills Opportunities
Employment Opportunities

Send Credential

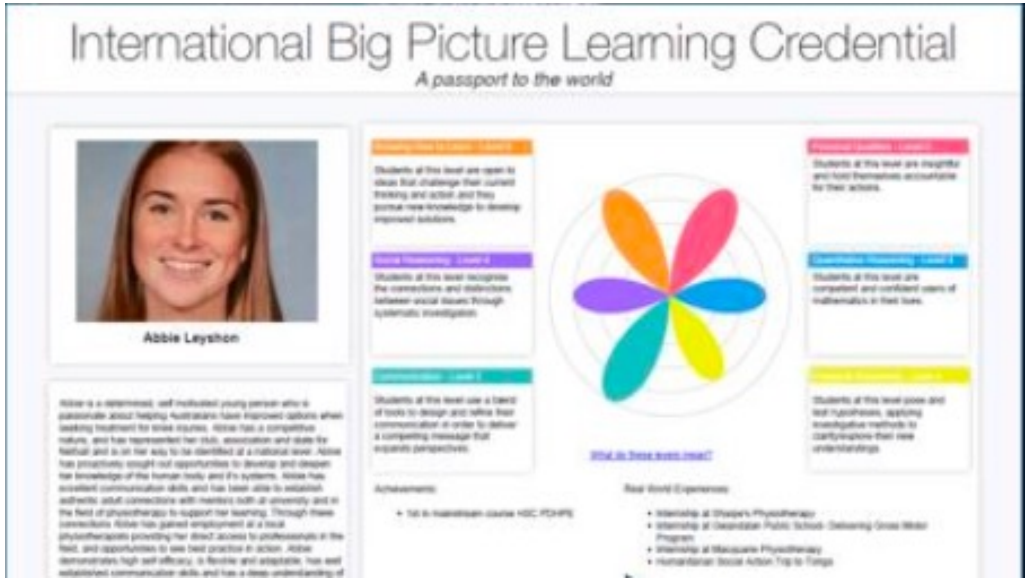
Verified Credentials

Send Skills Portfolio

Issue Verified Skills Credential

Registration Details
Personal Details
Organization Details
Course Details
Credential Details
Skills (vocational) Details

Job Seeker Personal Details
Job Seeker Education Details
Job Seeker Skills Details



International Big Picture Learning Credential

A passport to the world

Abbie Leyshon

Thank You

Questions?

beth@connect-edtech.com
@bethmhavinga

www.connect-edtech.com