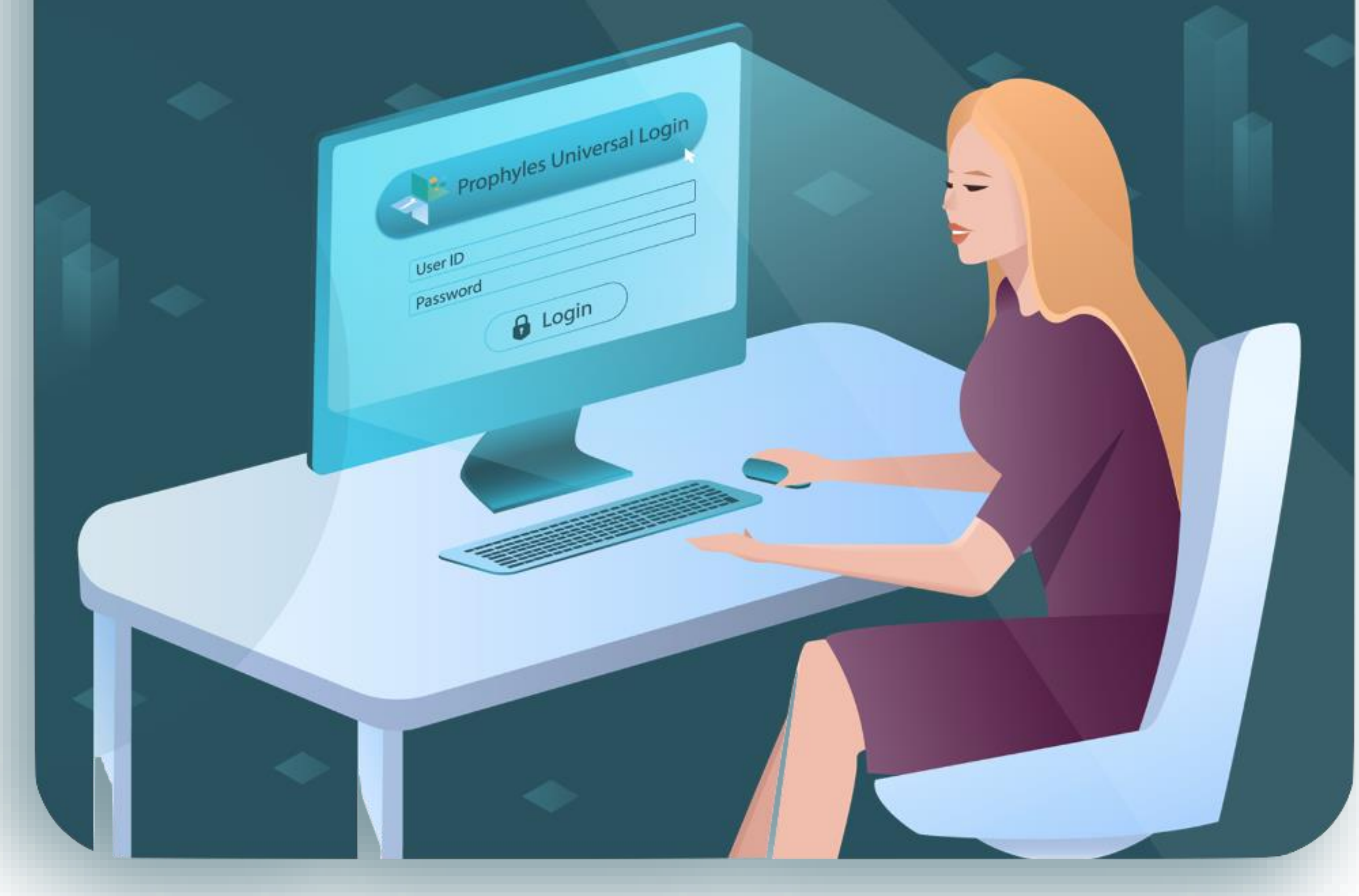
Prophyles

CYBERSECURITY

HOW A HACKER CRACKED A CNN CORRESPONDENT'S PASSWORDS

What’s wrong with logins? Everything!!!



Prophyles

What’s Wrong with Logins

Everything!!!

There are six major types of authentications:

User ID & Password

Multi-Factor

Biometric

Certificate

Token

Blockchain

How a Hacker Cracked a CNN Correspondent’s Passwords

User ID & Password Authentication

The User ID & Password Authentication method is currently the most common, and the least expensive, but the least secured. This method has two parameters: User ID and Password. The user ID is typically a unique identifier such as an email address or a phone number, which makes User IDs easily identifiable by hackers. The second parameter, the password, is not any safer because:

- If you make your password easy to remember, then it will be easily hacked, and vice versa, if you make it hard to hack, it will be hard to remember.

- If you use the same password everywhere, then you will significantly increase your probability to be hacked because your Personal Information would be sprinkled everywhere, but if you use a different password for every website, then you will have difficulty to remember them all.

- If you change your passwords often as you are advised to do, then you will have hard time remembering them all, but if you don’t change your passwords often, then you increase your probability to be hacked.

- If you use Keychains to remember all your passwords, and if you are hacked, then all the websites that you have signed up to will be compromised.

- If you use your browser cookies to automatically log in to any website, then you might as well not have a password at all.

- Even though Password Managers are temporary band-aids, they do mitigate some vulnerabilities and offer some warnings and alerts of potential data leaks, breaches, and attacks. However, they present the following risks:

    - Vulnerable centralized database where the passwords are stored
    - Crash of the application itself which causes users not to be able to log in.
    - Dependency of the vendor’s support.
    - Reliability of the vendor of the application who may go out of business.

What’s Wrong with Logins

Everything!!!

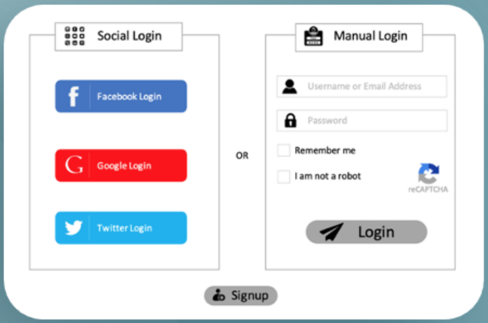
The User ID & Password Authentication offers two methods:

- **Manual Logins**

  Manual Logins are a pain – you first need to sign up, which means you are sprinkling your Personal Information everywhere you sign up. Thereafter, you need to manually type in your User ID and your Password. Once you do, then you will run into the problems mentioned above. In addition, the great majority of websites don’t have strong defenses against hackers. So, proprietary logins from the great majority of websites are dangerous.

- **Social Logins**

  With millions of people having already an account with one of the big tech firms, Social Logins came to the seen to appease some of the users’ frustrations with signups. However, their convenience, which we were craving, came at the expense of our privacy. Specifically:



  - Even though large websites have stronger defenses than the great majority of websites, however, they are very high target to hackers who routinely attack them. Just last week, Facebook admitted that more than 1 million accounts have been hacked. The largest hack was from 2013 to 2016 when 3 billion Yahoo! accounts were hacked. So, the probability for your Facebook, Google, Twitter, or LinkedIn account to be hacked some day is highly likely, if not already.

  - We got tricked by some social media firms in believing their slogans like *“Do No Evil”*, only to then realize that they were all along THE evil with their tracking and tracing capability that they sneakily hidden from us. Second to cookies, social logins are the biggest threat to our privacy that led to the creation of the “Surveillance Economy” that exploits *Residual Data* and *Derivative Data* which we leave behind while surfing the web that tech firms pick up as the raw material to package us as their product for sale to their customers – the advertisers.

Multi-Factor Authentication (MFA)

The Multi-Factor Authentication (MFA) forces users to pass some additional obstacles consisting of multi steps in order to log in. These factors represent an extra layer of security on top of the standard User ID & Password login. In addition to the User ID & Password, users must also submit a second factor such as a one-time code sent by email or text to users who wish to log in. For improved security, most large companies use MFA combined with the conventional User ID & Password login. Google, Microsoft, and Authy are the top three leading providers of MFA services. Since most attacks are done by bots, MFA is relatively secured but not bullet proof. In addition, MFA is difficult to set up and inconvenient to users, especially when the authentication is done on different devices. For example, have you ever tried to authenticate yourself on your smartphone to use Microsoft 365?!!!

Biometric Authentication

Biometric Authentication consists of recognizing a user's physical attributes such as fingerprint, palm, retina, face, or voice. The process includes two steps:

1. First, the physical characteristics of individuals are saved in a database – a vulnerability that Blockchain Authentication would address as discussed below.

2. Second, individuals' physical features are checked against the data contained in the database whenever a user wants to access any device or physically enter any premises. Biometric Authentication is mostly used in building, schools, airports, courts, etc. Recently, smartphones manufacturers like Apple and Samsung have implemented face and fingerprint recognitions to unlock their device.

Certificate Authentication

Certificate Authentication identifies people, servers, workstations, and devices by using an electronic digital identity such as SSL, which would be the equivalent to a driver's license or a passport. A certificate includes a user's digital identity consisting of a public key and a digital signature. This certificate verifies that the public key and the person who issued the certificate are both the same person. Before logging in, users must first present their digital certificate. In order to grant access, the private key and the certificate must match using cryptography.

Token Authentication

Token Authentication allows users to enter their credentials only once and obtain in return a digital *"token"* which is a unique encrypted string of characters and numbers. Thereafter, users don't have to input their login credentials every time they log in. The digital token essentially identifies the user who is requesting access. Most use cases, such as RESTful APIs which are accessed by many frameworks and clients, require Token Authentication.

Blockchain Authentication

Blockchain Authentication refers to methods of authentication that rely on blockchain for security. To date, most cryptocurrencies such as Bitcoin uses Blockchain Authentication in order to identify users. Because of its distributed and decentralized architecture, Blockchain inherently offers a much higher security compared to a centralized database because it is much harder to hack millions of nodes in a network versus hacking a single database. However, that does not mean that Blockchain is full proof of any potential attacks, but it is indeed the safest method.

Miscellaneous Authentications

In addition to the above main methods of authentications there are some subsets and variations such as Single Sign-On (SSO) Authentication, Adaptive Authentication, API Authentication, HTTP Basic Authentication, and API Authentication such as OAuth which is one of the most popular.