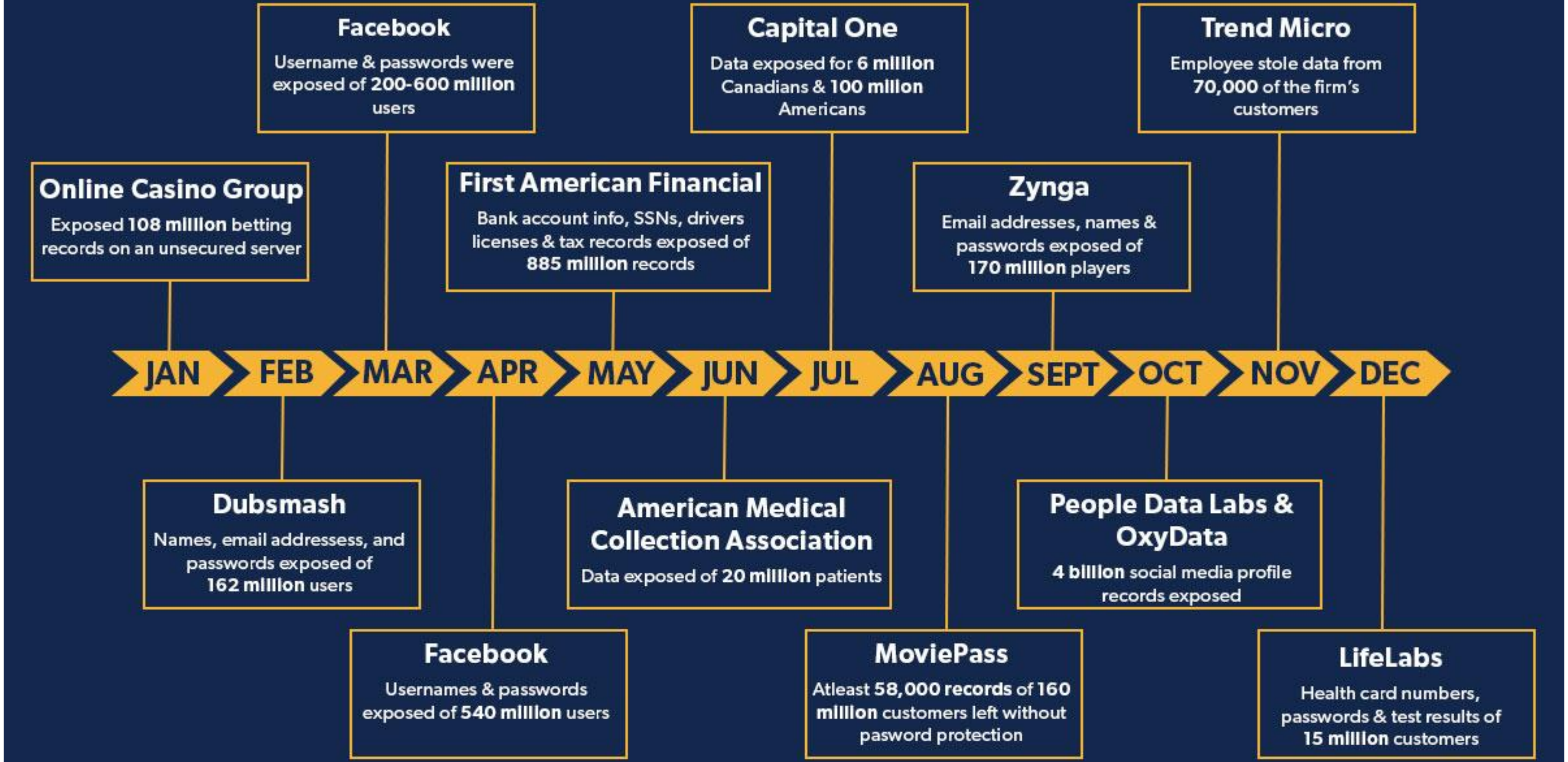
Managing Your Passwords

A Big Problem that we tend to ignore

Most Impactful Data Breaches of 2019

MEDIA S(•)NAR



JAN FEB MAR APR MAY JUN JUL AUG SEPT OCT NOV DEC

Online Casino Group

Exposed **108 million** betting records on an unsecured server

Dubsmash

Names, email addresses, and passwords exposed of **162 million** users

Facebook

Username & passwords were exposed of **200-600 million** users

Facebook

Usernames & passwords exposed of **540 million** users

First American Financial

Bank account info, SSNs, drivers licenses & tax records exposed of **885 million** records

American Medical Collection Association

Data exposed of **20 million** patients

Capital One

Data exposed for **6 million** Canadians & **100 millon** Americans

MoviePass

Atleast **58,000 records** of **160 million** customers left without pasword protection

Zynga

Email addresses, names & passwords exposed of **170 million** players

People Data Labs & OxyData

4 billion social media profile records exposed

Trend Micro

Employee stole data from **70,000** of the firm's customers

LifeLabs

Health card numbers, passwords & test results of **15 million** customers

Some of the 2020 Data Breaches

- Estee Lauder – 440 million records including plain text email addresses
- WishBone – 40 million user records with email and some passwords
- T-Mobile – names and phone numbers
- MGM Resorts – 142 million users names, addresses, phone numbers, birthdates

What’s Going On

- Throughout 2020, hackers increased their activity by more than 600%. This increase in activity affects older people more than other age groups, as they’re more likely to fall for email phishing scams. People over 60 account for nearly a quarter of the money lost through cyberattacks each year.
- Hackers have been responsible for over 4,000 attacks each day during 2020. There will have been over 1,460,000 attacks by the end of the year 2020. Nearly 90% of successful attacks occur thanks to human error, either by the target themselves or a third-party.

Who are these hackers?

1. Very sophisticated individuals or groups of individuals that earn their living “mining” information from large governments and corporations.
   A. Information is organized and sold on the “dark web”

      Or

   B. Given to their government sponsor
2. Small groups or individuals that purchase information from the “dark web” and use it to earn (or supplement) their living by scamming small organizations and individuals (ie. us!)

How do the “small guys” attack us?

1. Purchase phone numbers and call us with a scam
2. Purchase email lists and email us with a scam
    - Direct scam (get money directly from you)
        - “I’m your grandson, please send me money”
        - “I’m an organization that helps needy kids, please send us money”
        - “I have taken control of your computer, I know your password is “abc” and I know your secret, if you don’t send me $5,000 I’ll let everyone know”
    - Phishing (two step process, get your password by phishing, then purchase products from your account)
        - “Someone placed this order, please sign in here and verify this is your order”
        - “Your account is not secure, please sign in here and correct”
3. Use Malware to infect your browser and get you to phone a “support number”

The “personal” a “small guys” can attack us!

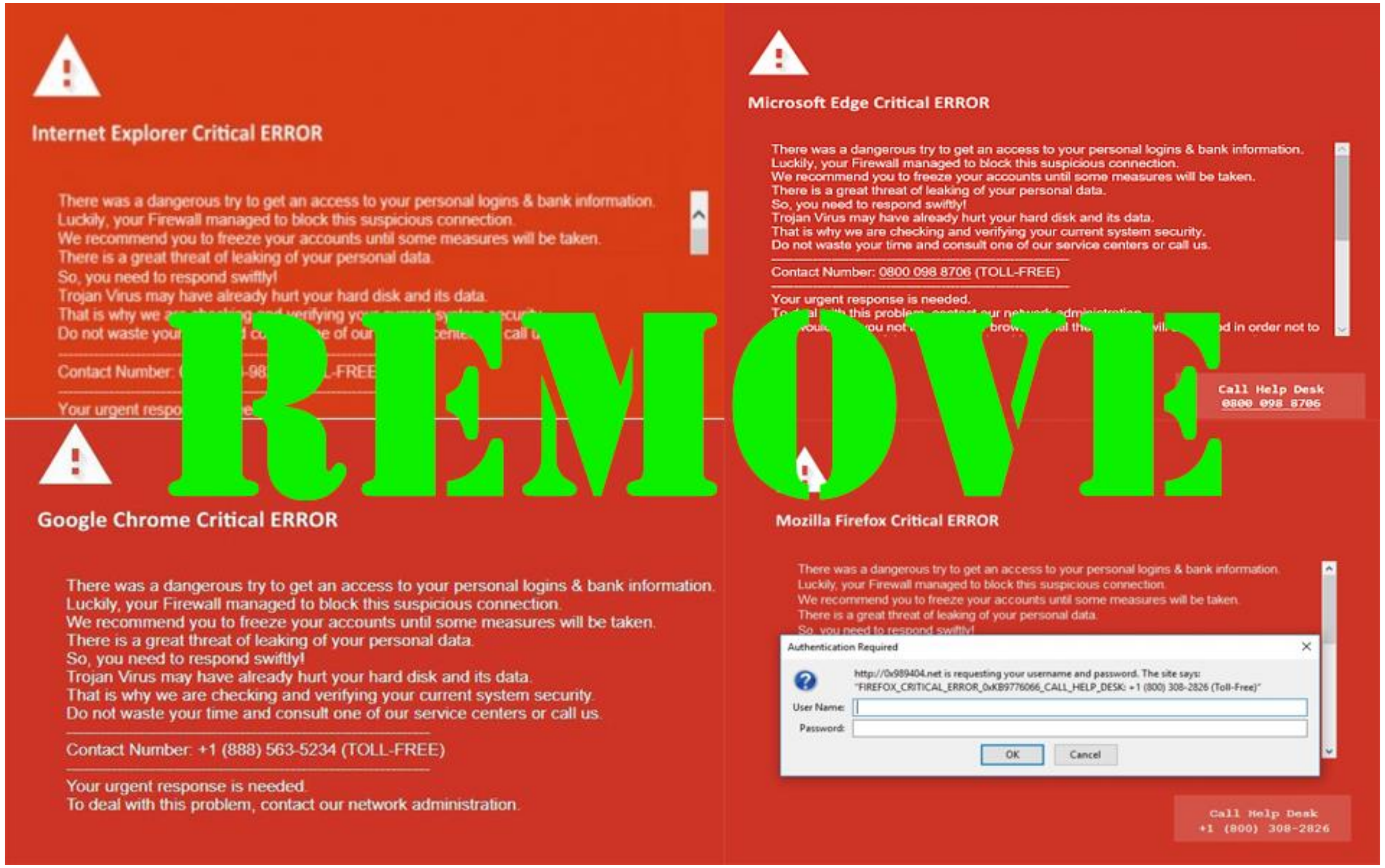
- Purchase a list that is organized
  - First and Last Name
  - Username and password
  - Birth date
  - Street address
- Spend the evening using a username and password to try logging into every website they think they can easily make money from
- Validate themselves when they succeed
- Send themselves gift cards or “whatever”

The first place they will go is your email – if they can get in there, they will have a very profitable night!

Two Common Attacks We See

- Malware from a website
  - Installed in website through a bogus advertisement
  - Infects the **browser** we are using : settings & add ons
  - Can only infect your **PC** if it asks for “permission to install”
- Phishing
  - An email or text with links that are not what they say they are
  - Following the link can lead to Malware or theft of identity information

Malware on a Website



Internet Explorer Critical ERROR

There was a dangerous try to get an access to your personal logins & bank information.
Luckily, your Firewall managed to block this suspicious connection.
We recommend you to freeze your accounts until some measures will be taken.
There is a great threat of leaking of your personal data.
So, you need to respond swiftly!
Trojan Virus may have already hurt your hard disk and its data.
That is why we
Do not waste your

Contact Number:

Your urgent respo

Microsoft Edge Critical ERROR

There was a dangerous try to get an access to your personal logins & bank information.
Luckily, your Firewall managed to block this suspicious connection.
We recommend you to freeze your accounts until some measures will be taken.
There is a great threat of leaking of your personal data.
So, you need to respond swiftly!
Trojan Virus may have already hurt your hard disk and its data.
That is why we are checking and verifying your current system security.
Do not waste your time and consult one of our service centers or call us.

Contact Number: 0800 098 8706 (TOLL-FREE)

Your urgent response is needed.

Google Chrome Critical ERROR

There was a dangerous try to get an access to your personal logins & bank information.
Luckily, your Firewall managed to block this suspicious connection.
We recommend you to freeze your accounts until some measures will be taken.
There is a great threat of leaking of your personal data.
So, you need to respond swiftly!
Trojan Virus may have already hurt your hard disk and its data.
That is why we are checking and verifying your current system security.
Do not waste your time and consult one of our service centers or call us.

Contact Number: +1 (888) 563-5234 (TOLL-FREE)

Your urgent response is needed.
To deal with this problem, contact our network administration.

Mozilla Firefox Critical ERROR

There was a dangerous try to get an access to your personal logins & bank information.
Luckily, your Firewall managed to block this suspicious connection.
We recommend you to freeze your accounts until some measures will be taken.
There is a great threat of leaking of your personal data.
So, you need to respond swiftly!

Authentication Required

http://0x989404.net is requesting your username and password. The site says: "FIREFOX_CRITICAL_ERROR_0xKB9776066_CALL_HELP_DESK: +1 (800) 308-2826 (Toll-Free)"

User Name:

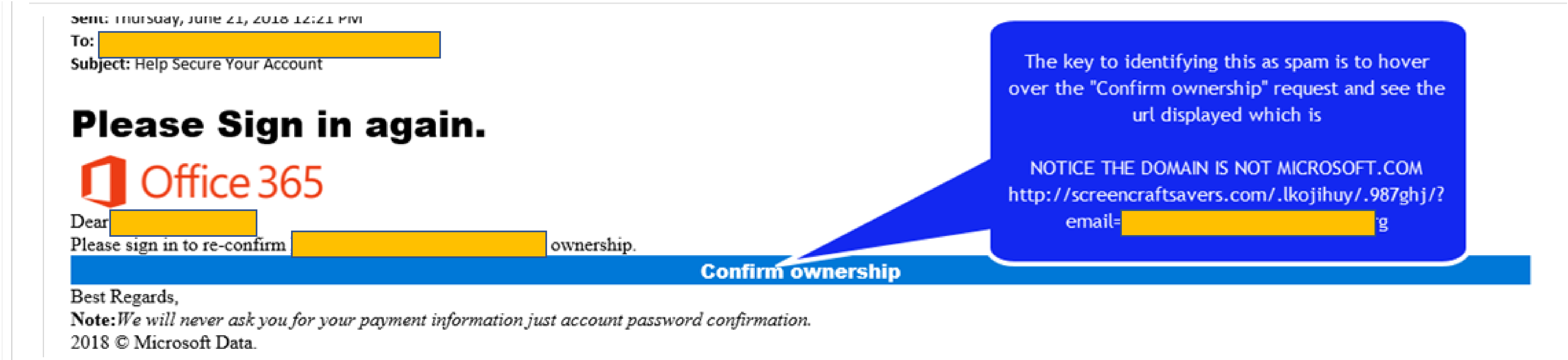
Password:

Actions

- Do not call any numbers given
- Do not click any links
- Do – Close the browser tab!
    - Hit Esc key and then close the browser
    - Go to Task Manager and close all the occurrences of the browser
    - Power off by holding the power button down 30 seconds, then restart

      If the browser still is locked
    - Power off and bring the PC to the Resource Center for a volunteer to work with.

Phishing



Sent: Thursday, June 21, 2018 12:21 PM
To: [redacted]
Subject: Help Secure Your Account

Please Sign in again.

Office 365

Dear [redacted]
Please sign in to re-confirm [redacted] ownership.

Confirm ownership

Best Regards,
Note: *We will never ask you for your payment information just account password confirmation.*
2018 © Microsoft Data.

The key to identifying this as spam is to hover over the "Confirm ownership" request and see the url displayed which is

NOTICE THE DOMAIN IS NOT MICROSOFT.COM
http://screencraftsavers.com/.lkojihuy/.987ghj/?email=[redacted]

How do we protect ourselves?

- Recognize that your name, email address and password are worth money and probably are for sale on the dark web!
- Manage your usernames and passwords well, so that the information about you is not correct!
  - Do not use a password more than once
  - Change your passwords periodically on your most important services:
    - Your email address
    - Your bank
    - Amazon
  - Keep track of **ALL** of your usernames and passwords so you can change them if you are hacked **and use them when you have a new device** ☺

How do I Manage My Usernames and Passwords?

1. Decide to spend time doing it.

   “pay me now or pay me later”

   This is more important than cleaning your garage

2. Choose a Process for doing it.

   Manual

   Semi-Automated

   Automated (a password management system)

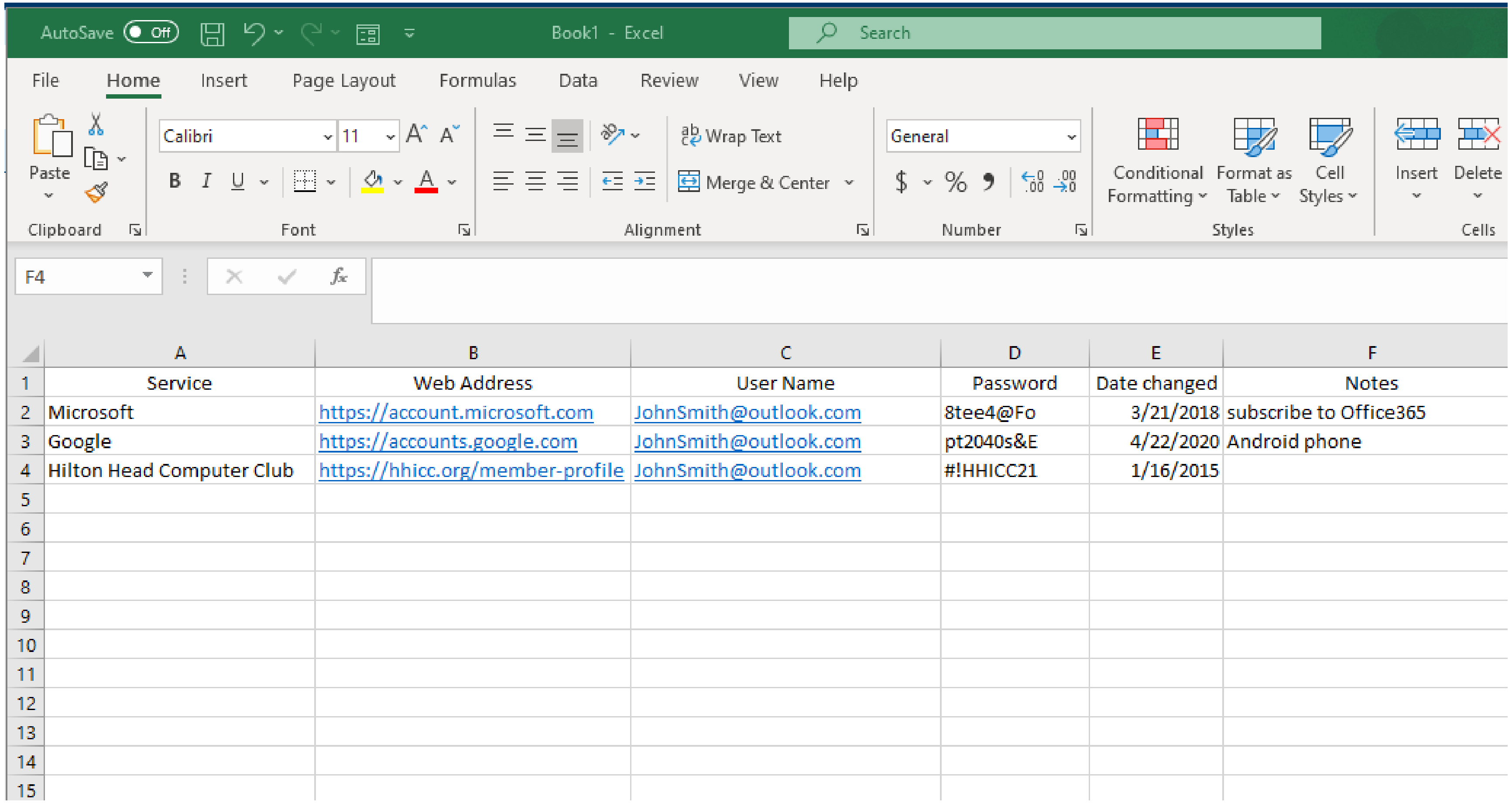
3. Do it!

Manual

- **First Habit** – never enter a new password without writing it down first and then enter the password reading it from what you wrote.
  - Passwords should be at least 8 characters and include capital and lower-case letters as well as a number or two and a special character
  - You wouldn’t believe how quickly you can forget if the particular letter was a capital or lower-case!
- After you have changed the password, write the name of the service, the username and the password in a ledger that is organized by service.
  - Put a line through or erase the last password for this service
  - Keep the ledger somewhere that isn’t totally obvious, but your spouse or kids know where it is

Semi-Automated

Use a spread sheet or Word Processor to build a table – encrypt the table when saved



	A	B	C	D	E	F
1	Service	Web Address	User Name	Password	Date changed	Notes
2	Microsoft	https://account.microsoft.com	JohnSmith@outlook.com	8tee4@Fo	3/21/2018	subscribe to Office365
3	Google	https://accounts.google.com	JohnSmith@outlook.com	pt2040s&E	4/22/2020	Android phone
4	Hilton Head Computer Club	https://hhicc.org/member-profile	JohnSmith@outlook.com	#!HHICC21	1/16/2015	
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						

Automated

- Use a Password Management app
  - Stores passwords and makes them available across devices
  - Can create strong passwords
  - Stored in the cloud so available anywhere
- Highly rated apps
  - LastPass : https://www.lastpass.com
  - 1Password : https://1password.com
  - RoboForm : https://roboform.com
  - Apple Keychain

Note: Most browsers will remember passwords – DO NOT DEPEND on this

Pros and Cons

Manual	Semi-Automated	Automated
Free	Free	Some charges
Easy	Can store in the cloud	Automatic logins on devices
You may have to carry it with you sometimes	Need to know how to use a spreadsheet and encrypt it	Can use it anywhere
Big trouble if you lose it	If you forget the encryption key you are in big trouble	You need to learn to use it and if you forget your username and password you are in big trouble
Must protect it physically – low chance a burglar will be looking for it	Protected by encryption and where you keep it – low chance any hacker will spend time looking for it	Protected by corporation security – but obvious place for big hackers to try and hack

Other Safety Mechanisms

- Two Step (Factor) authentication
  - Username and Password to login to a service
  - Service texts a code to your phone

    Or
  - An email to your email address

Should use this in any financial system you have access to

- Biometrics – Finger print, facial recognition

Identity Theft Tracking and Insurance

IdShield idshield.com

Transunion, Equifax and Experian credit monitoring and alerts

Covers you, your spouse or domestic partner and up to 10 dependent children

Comprehensive privacy and ID protection

Unlimited Consulting

$1M Identity Theft Protection Coverage

12 Month Credit Score Tracking History

24/7 Access to Customer Support

Unlimited Identity Restoration Services

Access to In-house Licensed Private Investigators

Access to In-house Licensed Private Investigators

24/7 Credit Monitoring and Alerts

Dark Web Surveillance

Bank account monitoring

Payday Loan Monitoring

Credit Report Disputes

Sex Offender Alerts

Court Records & Bookings

Social Security Number Monitoring

Other Highly Rated Services

- Identity Guard
- LifeLock
- Experion