Social Media Security

BANK OF THE WEST
BNP PARIBAS

Corporate Security | Cybersecurity

June 2018

Table of Contents

- Why should I care about Social Media Security?

- Can Social Media really be used in malicious ways?

- How can I protect myself and my organization?

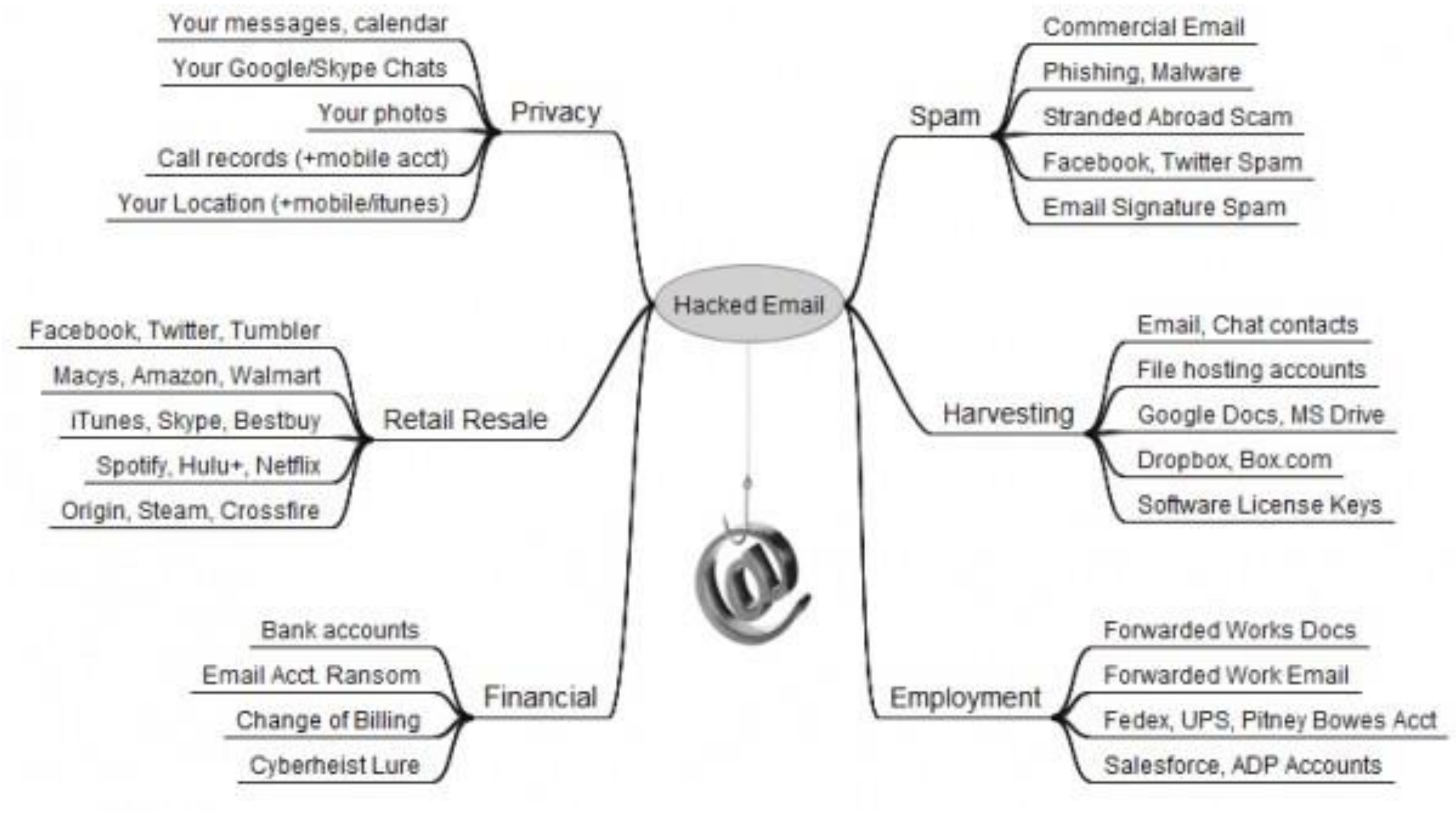
Why should I care about Social Media Security?

You have value (your accounts)

- Financial accounts (Bank, Retirement, Credit Card, etc..)
- $8 iTunes account
- $6 Fedex.com, Continental.com and United.com
- $5 Groupon.com
- $4 Godaddy.com, ATT.com, Sprint.com, Verizonwireless.com, Tmobile.com
- $2.50 Facebook and Twitter
- $1 to $3 Dell.com, Overstock.com, Walmart.com, Tesco.com, Bestbuy.com, Target.com

Source: krebsonsecurity.com

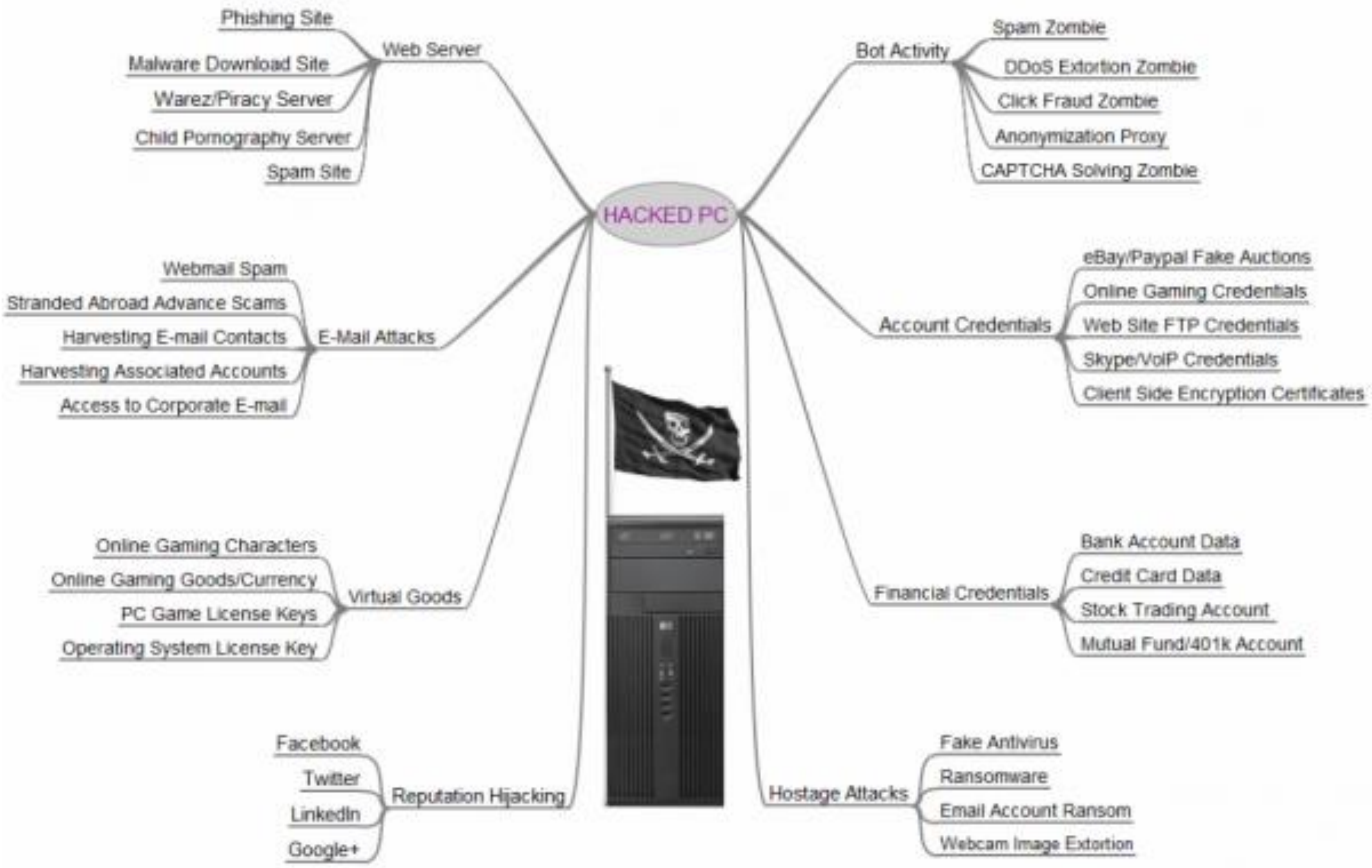
You have value (your email account)



BANK OF THE WEST
BNP PARIBAS

Source: krebsonsecurity.com

You have value (your computer)

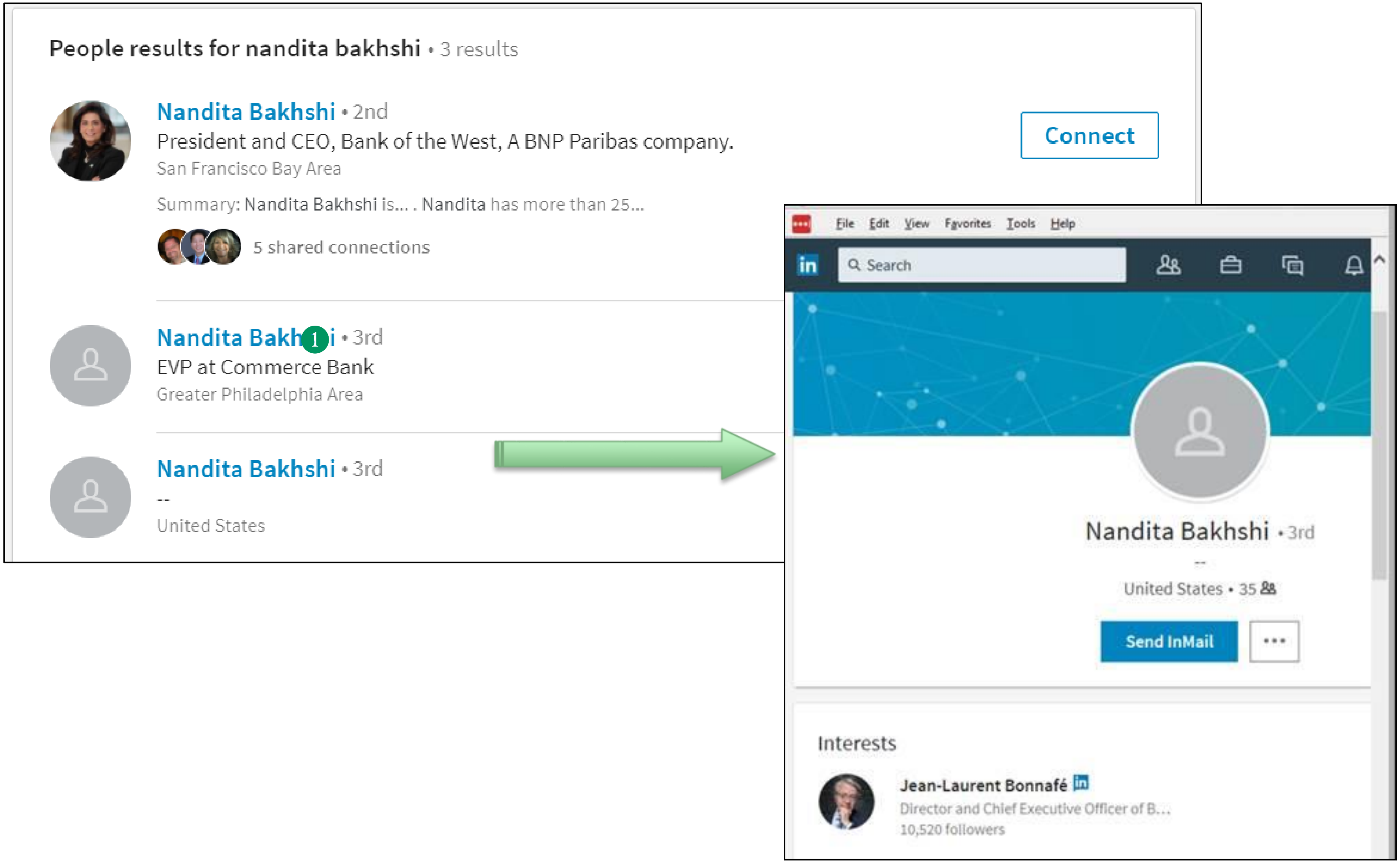


BANK OF THE WEST
BNP PARIBAS

Source: krebsonsecurity.com

How can Social Media be used maliciously?

Gain Trust



People results for nandita bakhshi • 3 results

Nandita Bakhshi • 2nd
President and CEO, Bank of the West, A BNP Paribas company.
San Francisco Bay Area
Summary: Nandita Bakhshi is... . Nandita has more than 25...
5 shared connections

Connect

Nandita Bakhshi • 3rd
EVP at Commerce Bank
Greater Philadelphia Area

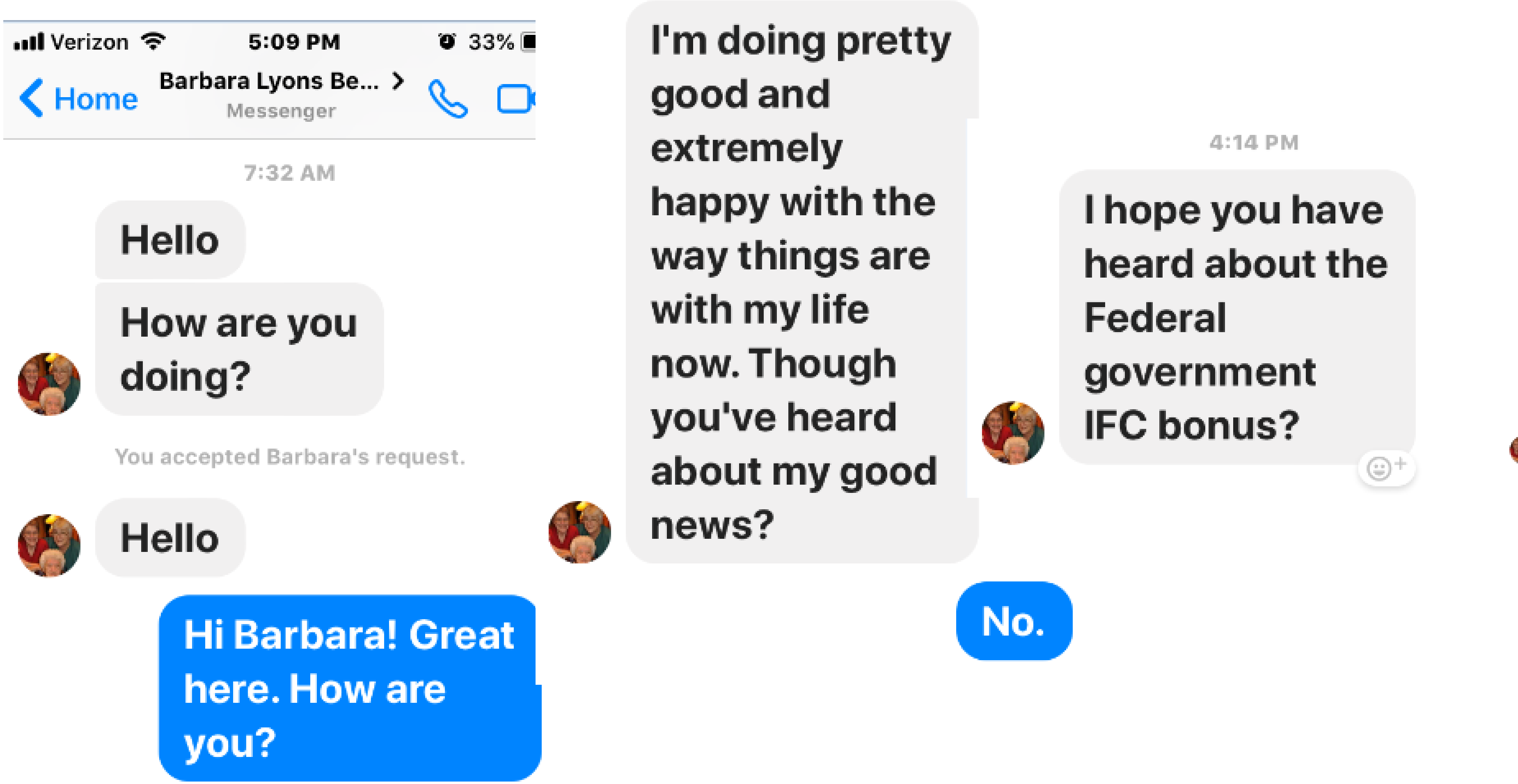
Nandita Bakhshi • 3rd
--
United States

Nandita Bakhshi • 3rd
--
United States • 35

Interests

Jean-Laurent Bonnafé
Director and Chief Executive Officer of B...
10,520 followers

Misuse trust to sell, steal, defraud, infect



Verizon 5:09 PM 33%

< Home Barbara Lyons Be... > Messenger

7:32 AM

Hello

How are you doing?

You accepted Barbara's request.

Hello

Hi Barbara! Great here. How are you?

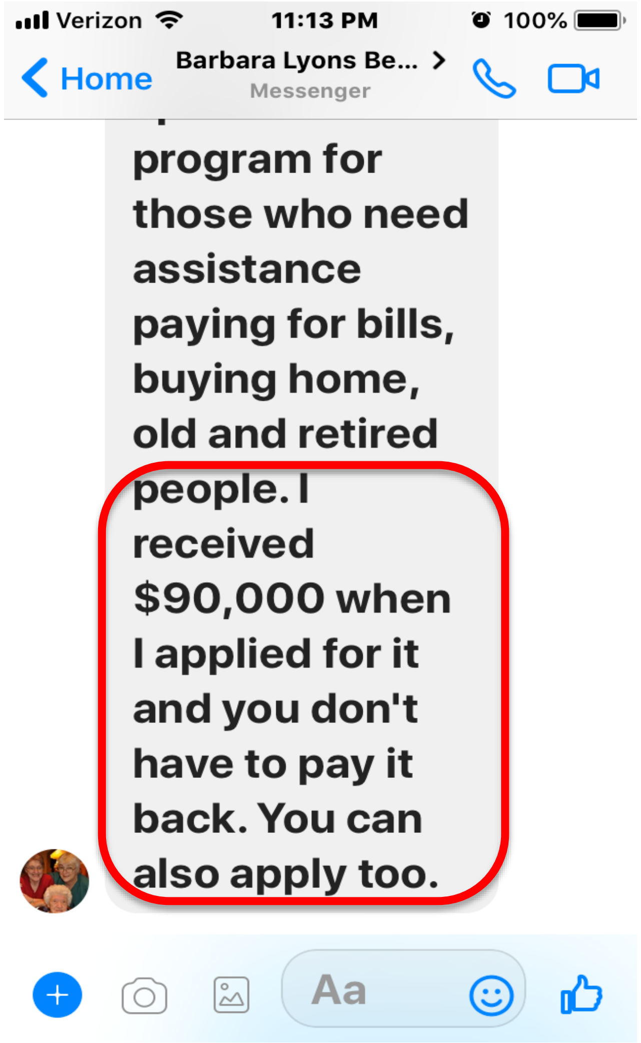
I'm doing pretty good and extremely happy with the way things are with my life now. Though you've heard about my good news?

4:14 PM

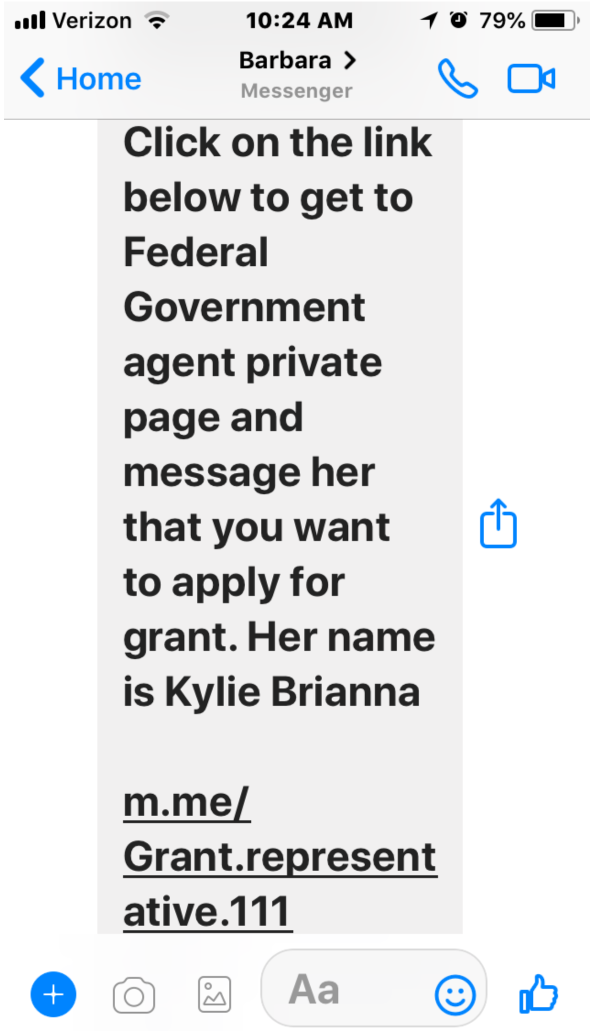
I hope you have heard about the Federal government IFC bonus?

No.

Misuse trust to sell, steal, defraud, infect



program for those who need assistance paying for bills, buying home, old and retired people. I received $90,000 when I applied for it and you don't have to pay it back. You can also apply too.



Click on the link below to get to Federal Government agent private page and message her that you want to apply for grant. Her name is Kylie Brianna

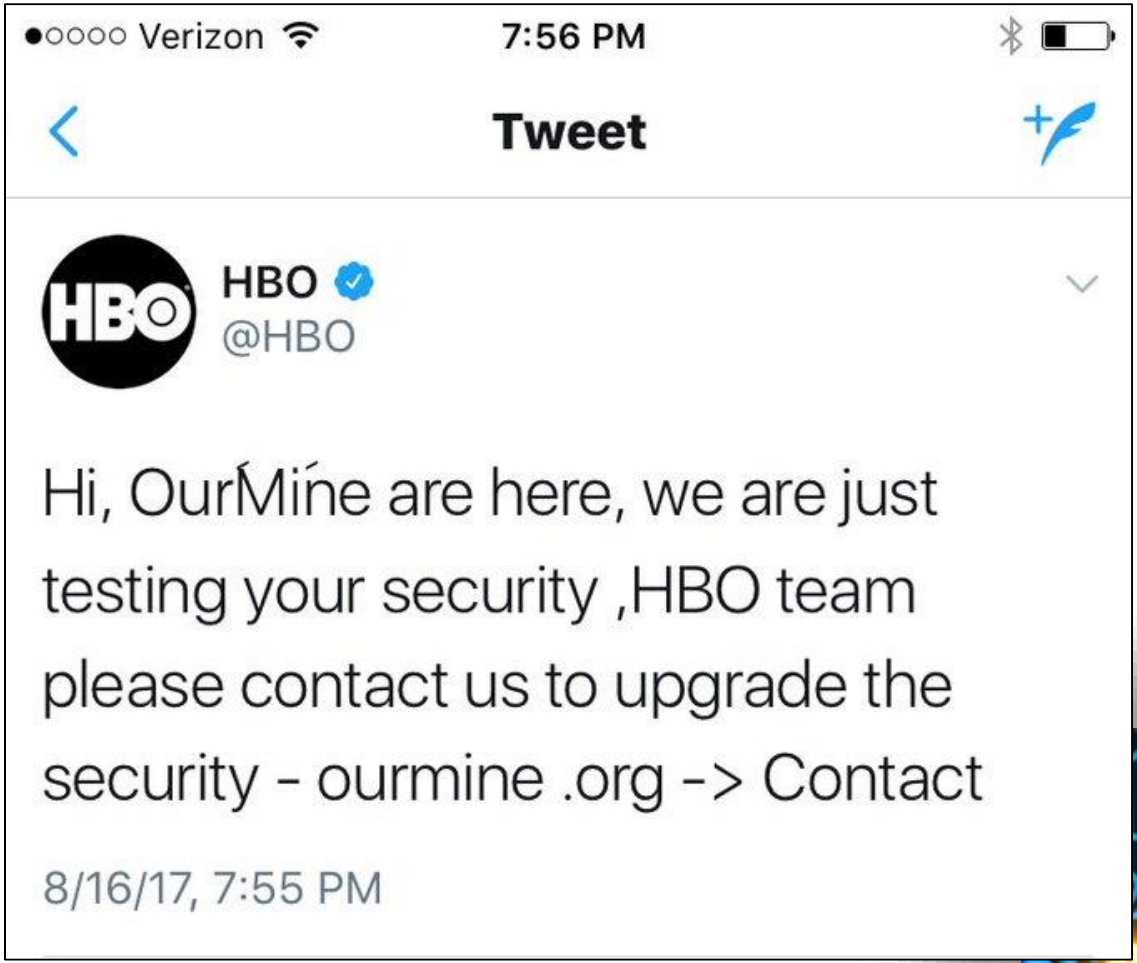
m.me/Grant.representative.111

BANK OF THE WEST
BNP PARIBAS

Burglary

Source: https://www.marketwatch.com/story/6-lessons-we-can-learn-from-kim-kardashians-robbery-2016-10-03

Public Embarrassment #1



●○○○○ Verizon 7:56 PM

Tweet

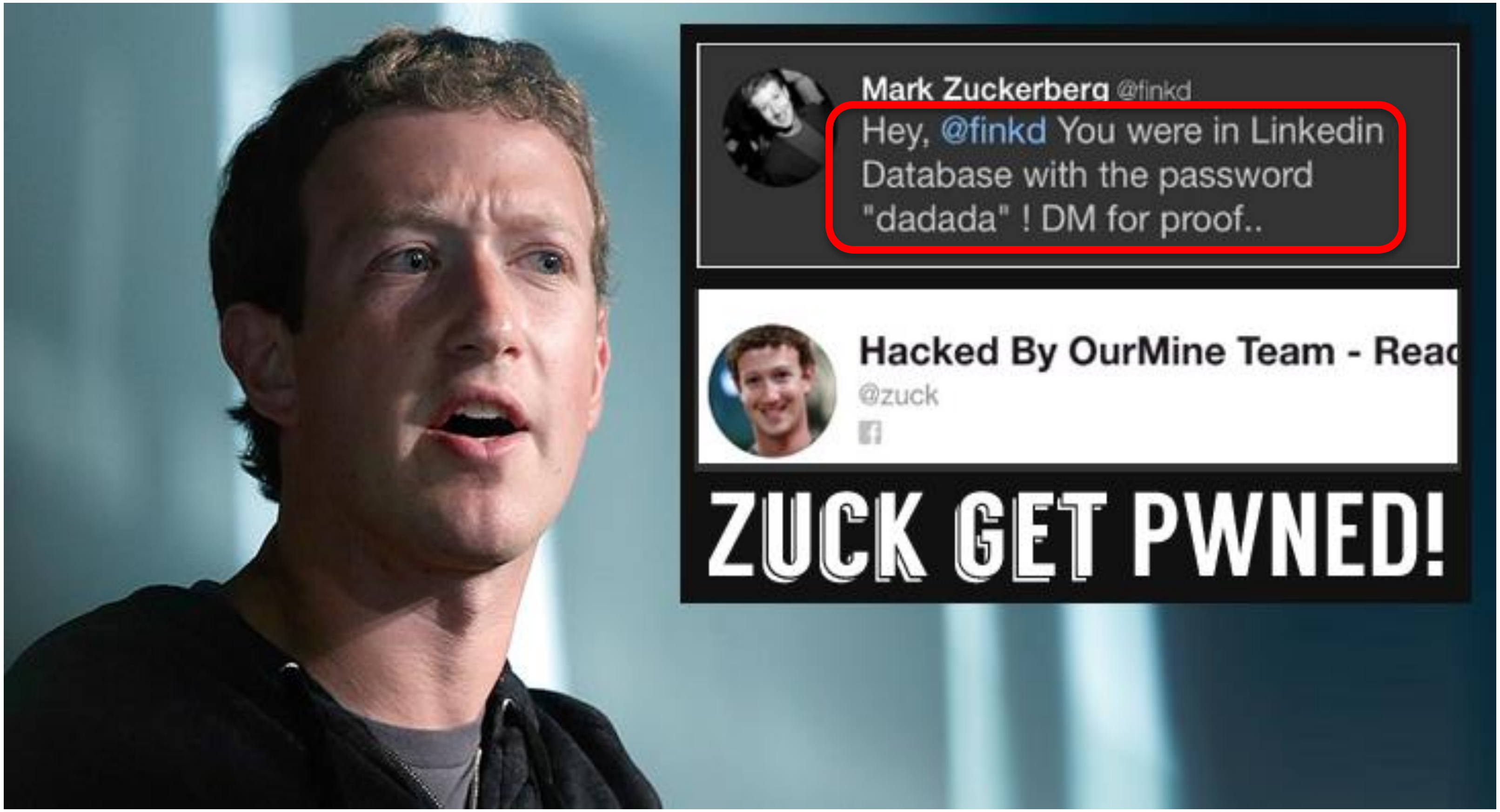
HBO
@HBO

Hi, OurḾińe are here, we are just testing your security ,HBO team please contact us to upgrade the security - ourmine .org -> Contact

8/16/17, 7:55 PM

Source: https://www.engadget.com/2017/08/17/hbo-hack-social-media/

Public Embarrassment #2



Mark Zuckerberg @finkd

Hey, @finkd You were in Linkedin Database with the password "dadada" ! DM for proof..

Hacked By OurMine Team - Reac

@zuck

Source: https://arstechnica.com/information-technology/2016/06/mark-zuckerberg-twitter-pinterest-hacked/

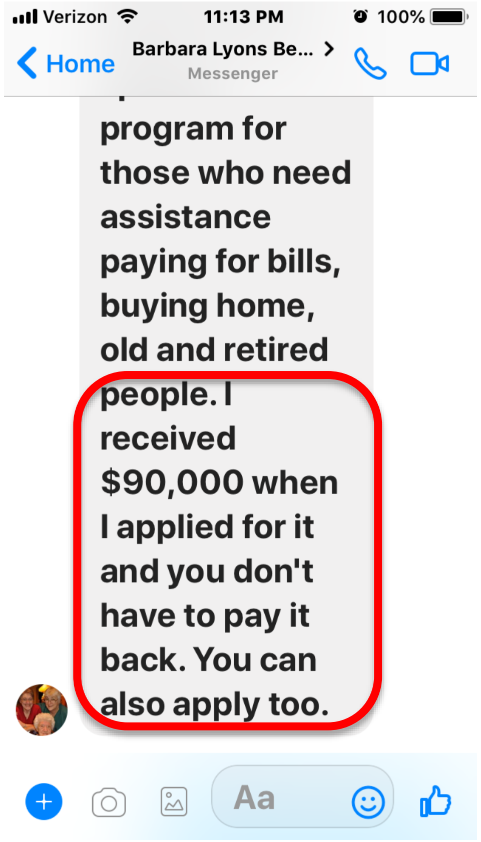
How can I protect myself and my organization?

Be suspicious

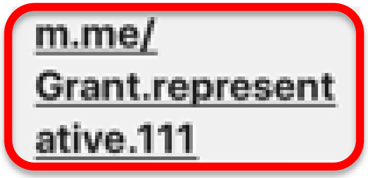
1. If something sounds too good to be true, it probably is!

2. Don't click on links or attachments from unknown persons

3. Don't click on links or attachments from <u>known persons</u> under suspicious circumstances



program for those who need assistance paying for bills, buying home, old and retired people. I received $90,000 when I applied for it and you don't have to pay it back. You can also apply too.



m.me/Grant.representative.111

Be careful what you share on social media!

1. Keep valuables off social media. Anyone who posts photos of expensive possessions could be putting themselves at a higher risk of being robbed.

2. Do not advertise that you are going out of town. Social media can be used to discern when homeowners are traveling, allowing burglars to know the premises are empty and unprotected. Share details of your trip after you get home!

3. Be careful with geotagging. Tagging or sharing your location on social media can create a clear map to you, your family members and your valuables.

Protect your accounts

Mark Zuckerberg @finkd
Hey, @finkd You were in Linkedin Database with the password "dadada" ! DM for proof..

Hacked By OurMine Team - Read
@zuck

1. Create a strong passwords that are difficult to guess for accounts and devices

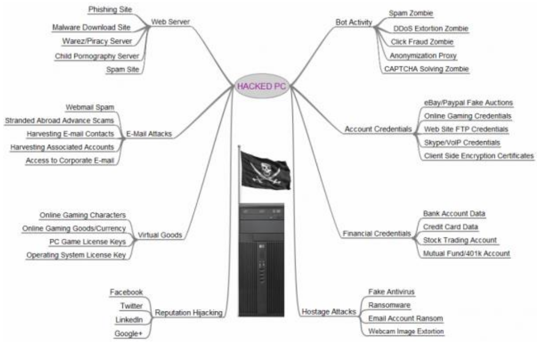
2. Develop a technique to make your passwords unique for every site

3. Consider using a password manager to keep track of them

4. Do not mix personal and business accounts

5. **Use two-factor authentication**

Protect your devices



1. Be vigilant.

2. Keep your devices patched.
   Anything that is connected!

3. Use security products and check
   that they are current.

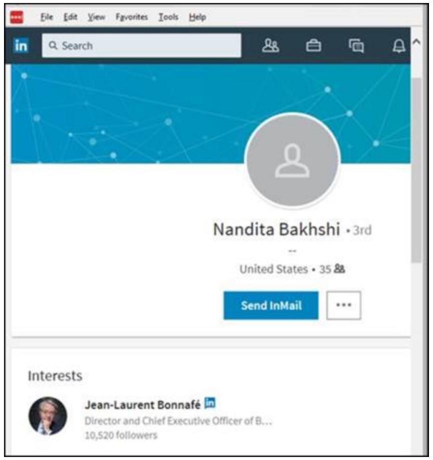
4. Educate yourself.

Protect Yourself From Fictitious Connection Requests

- Ensure the privacy and security settings for your social media sites are set to the appropriate preference level. For example, do you want your profile on LinkedIn to be public or private?

- If you have connected with an unsavory character, remember you can always unfriend or delete a connection on social networks.

- If you believe you've been a victim of a phishing scam or a cyber attack, quickly change your passwords and, if you feel it's necessary, close accounts.



Nandita Bakhshi • 3rd

--

United States • 35

Interests

Jean-Laurent Bonnafé

Director and Chief Executive Officer of B...

10,520 followers

Thank you!

Appendix

Ways to Protect Yourself

- Pick a strong password. Use a combination of at least six numbers, letters and punctuation marks (like ! and &). It should be different from other passwords you use elsewhere on the internet.
- Change your password regularly, especially if you see a message from Instagram asking you to do so. During automated security checks, Instagram sometimes recovers login information that was stolen from other sites.
- Never give your password to someone you don't know and trust.
- Turn on two-factor authentication for additional account security.
- Make sure your email account is secure. Anyone who can read your email can probably also access your Instagram account.
- Log out of Instagram when you use a computer or phone you share with other people. Don't check the "Remember Me" box when logging in from a public computer, as this will keep you logged in even after you close the browser window.

https://help.instagram.com/368191326593075

Ways to Protect Yourself

- Choose trusted and strongly encrypted wireless networks (Wi-Fi) or Virtual Private Networks (VPNs).
- If you ever suspect your account has been compromised, change your password right away by following these steps:
- Go to Settings -> Change Password and change your password
  - https://www.linkedin.com/help/linkedin/answer/2873/changing-your-password?lang=en

https://blog.linkedin.com/2011/05/23/user-security

https://safety.linkedin.com/staying-safe#Protecting-Yourself

Securing LinkedIn

Follow these simple steps to secure your LinkedIn profile:
Select who can send you invitations

- Edit communication settings so you can set select who can send you invitations with one of the following three message options below:
  - Anyone on LinkedIn
  - Only people who know your email address or appear in your "Imported Contacts" list
  - Only people who appear in your "Imported Contacts" list

- To select who can send you invitations, access the Privacy & Settings section of your profile. From the Privacy & Settings section click the **Communications tab** and chose Select who can send you invitations.

- Select the types of messages you're willing to receive
  - Within the Communications tab, click the Select the types of messages you are willing to receive link and modify InMail options like the partial list shown below:
  - Messages
    - Introductions, InMail and Open Profile messages (Recommended)
    - Introductions and InMail only
    - Introductions only

- Turn on/off your activity broadcasts
  - To prevent users from being alerted each time you make an edit to your profile, you can select the Turn on/off your activity broadcasts option.
  - To access this setting, from within the Privacy & Settings section of your profile, click the Profile tab.

Ways to Protect Yourself

1. Use a strong password that you don’t reuse on other websites.
2. Use login verification.
3. Require email and phone number to request a reset password link or code.
4. Be cautious of suspicious links and always make sure you’re on twitter.com before you enter your login information.
5. Never give your username and password out to third parties, especially those promising to get you followers, make you money, or verify you.
6. Make sure your computer software, including your browser, is up-to-date with the most recent upgrades and anti-virus software.

https://help.twitter.com/en/safety-and-security/account-security-tips

Ways to Protect Yourself

Following Three Security Options makes your Facebook Account Secure and Hack Proof.

1) Enable Login Notification to know when anybody (or a hacker) tries to login with your User ID and Password, you will receive a Notification on your cell phone and you will come to know that it's time to change your password right now because the hacker has got your password and is trying to log in to your Facebook Account.

To Enable Login Notification
Go to Home -> Account Settings -> Security -> Login Notification. Put a Check Mark on your preferred option and click Save Changes button.

2) Always check your Active Sessions.

If you notice any unfamiliar location or device, it means your Facebook Account is at risk. Just click on End Activity and don't forget to change your password after that.

To Check Active Sessions
Go to Home -> Account Settings -> Security -> Active Sessions.

3) Enable Secure Browsing to make your account more secure.
Go to Home-> Account Settings -> Security -> Secure Browsing.

Know more https://www.facebook.com/about/basics

Securing Facebook

Follow these simple steps to secure your Facebook profile:

- Click the down arrow on the far right at the top of the page. This is next to the Globe.
- Click Settings from the drop-down menu.
- Click Security from the menu on the left. Make sure Secure Browsing is enabled.
- Click Privacy from the menu on the left.
- Click Edit next to "Who can see your future posts?" and set to Friends.
  - This limits who can see what you post
- Click Limit Past Posts next to "Limit the audience for posts you've shared with friends of friends or public?"
  - This allows you to retroactively change the permissions on your posts. Click Limit Past Posts.
- Click Edit next to "Who can look you up using the email address or phone number you provided" and "Who can look up your timeline by name."
  - Select the setting you want from the drop-down menu. Recommend limiting to Friends or Friends of Friends, rather than Everyone. By doing so you automatically turn off the ability to be found and indexed by search engines such as Google.
- Click Use Activity Log next to "Review all your posts and things you're tagged in"
  - Identify every piece of content to do with you on Facebook one post at a time.
  - Includes your status updates, comments you've made on other people's status updates, things you've liked, apps you've used, photo's you're tagged in; basically everything Facebook and you.
- Click Timeline and Tagging from the menu on the left. Then Click Edit next to "Who can see posts you've been tagged in on your timeline". Select Friends, or even Only Me if you really want to lock things down.
- Click Edit next to " Who can see what others post on your timeline." Select Friends or even Only Me.
- Click Edit next to "Who sees tag suggestions when photos that look like you are uploaded?" Set the drop down menu to No One to prevent Facebook from auto suggesting you be tagged in photos.

Managing Application Access on Facebook

Cambridge Analytica reportedly gained access to data from Facebook users' accounts and wielded it to create a "psychological warfare" tool
Affected users' gave their consent to provide data to Cambridge Analytica when they signed up for the third-party app, thisisyourdigitallife.

Here's how to check your app settings on Facebook:

- On desktop, click the downward facing arrow in the upper-right side of your News Feed. Then, click "Settings." From there, tap "Apps" in the left-hand sidebar.
- On mobile, tap the icon showing three stacked lines. The icon is on top of your screen if you're using the Android app, and it's on the bottom if you're on iOS. Select "Settings." You may need to scroll down a bit to find it. Tap "Account Settings," then scroll down and tap "Apps." Select "Logged in with Facebook" to see the services accessing your account.
- You can now view the apps you have logged into with Facebook.
- Facebook has access to quite a bit of data, including relationship status, friend list, and birthday. Select "Remove App" to get rid of it.
- Take as much responsibility for yourself and your data as you can, because it impacts your friends, too. Review connected apps and remove some of them if you must.