ETHICAL HACKING: FOOTPRINTING AND VULNERABILITY ANALYSIS

EMMANUEL OKOI, B-TECH, CCNA, CEH,CSSA,CPENT
CYBER SECURITY ANALYST

01

WHOAMI

Just a brief description of me.

02

NETWORK INFORMATION GATHERING

Passive and Active Reconnaissance

03

VULNERABILITY ASSESSMENT

Vulnerability Identification

04

EMAIL SECURITY & SOCIAL ENGINEERING

Social Engineering Protection

05

SUMMARY

Just the wrap up of all discussed and questions.

3

ADVPHISH INSTALL/RUN

INSTALLATION

```
└──⍰ $ git clone https://github.com/Ignitetch/AdvPhishing.git
└──⍰ $ cd AdvPhishing/
└──⍰ $ chmod 777 *
└──⍰ $ ./Linux-Setup.sh
└──⍰ $ ./AdvPhishing.sh
```

AVAILABLE TUNNELLING OPTIONS

LOCALHOST

NGROK (https://ngrok.com/)

TO BE USED FOR EDUCATIONAL PURPOSES ONLY

4 EMAIL SECURITY AND SOCIAL ENGINEERING

Security is Everyone’s business and protecting our Digital Digital Identities should be a top priority to everyone and not just to Security Analyst.

Here, we’ll be treating Security measures in protecting our passwords, mails, and accounts from attacks like ***“Bruteforcing, Social Engineering, Password guessing, Phishing, e.t.c”***

…

95% of cybersecurity breaches are caused by human error. (Cybint)

48% of malicious email attachments are office files. (Symantec)

The top malicious email attachment types are .doc and .dot which make up 37%, the next highest is .exe at 19.5%. (Symantec)

…

1 PASSWORD SECURITY

- The idea of generating strong passwords cannot be overemphasized The best passwords will thwart brute force and dictionary attacks, but it's also possible to make them easy to remember. This article will build and enrich you with ideas to make your accounts unbreakable.

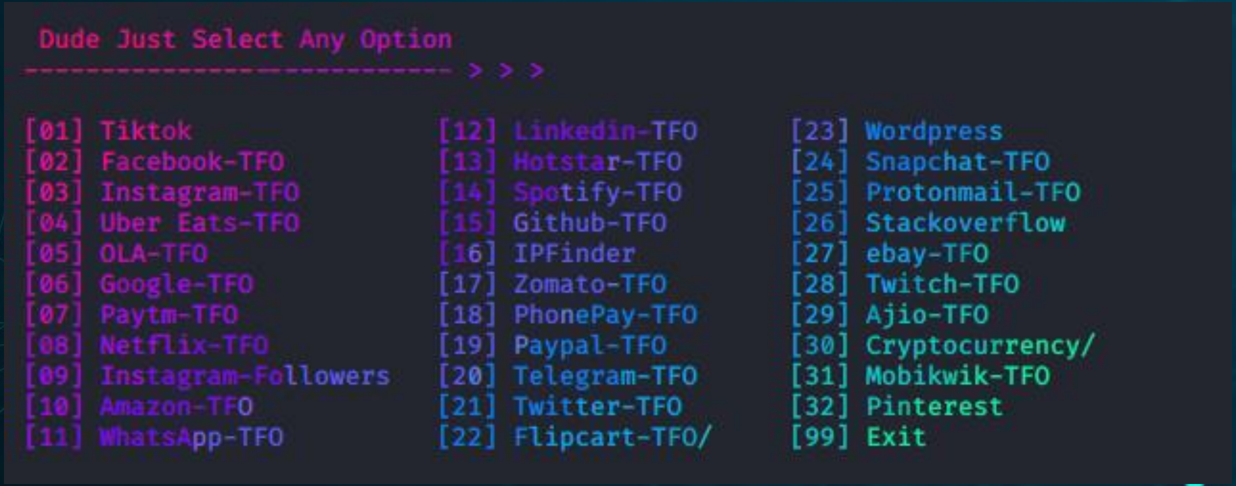
- The basic ways passwords are hacked are through
  - Brute-force attacks
  - Dictionary attacks
  - Phishing attacks

- To prevent your passwords from being hacked by social engineering, brute force or dictionary attack method, and keep your online accounts safe, you should carry out these best practices:

3 **PHISHING**

- **Tool : AdvPhishing**

As the name implies, it’s one of the most Advance phishing tools because of it extra features which includes {Phishing, IPGrabbing & Information Gathering, OTP Phishing}. It’s also known to have a more updated login pages of over 32 social media and payment platforms.



```
 Dude Just Select Any Option
---------------------------- > > >

[01] Tiktok                 [12] Linkedin-TFO        [23] Wordpress
[02] Facebook-TFO           [13] Hotstar-TFO         [24] Snapchat-TFO
[03] Instagram-TFO          [14] Spotify-TFO         [25] Protonmail-TFO
[04] Uber Eats-TFO          [15] Github-TFO          [26] Stackoverflow
[05] OLA-TFO                [16] IPFinder            [27] ebay-TFO
[06] Google-TFO             [17] Zomato-TFO          [28] Twitch-TFO
[07] Paytm-TFO              [18] PhonePay-TFO        [29] Ajio-TFO
[08] Netflix-TFO            [19] Paypal-TFO          [30] Cryptocurrency/
[09] Instagram-Followers    [20] Telegram-TFO        [31] Mobikwik-TFO
[10] Amazon-TFO             [21] Twitter-TFO         [32] Pinterest
[11] WhatsApp-TFO           [22] Flipcart-TFO/       [99] Exit
```

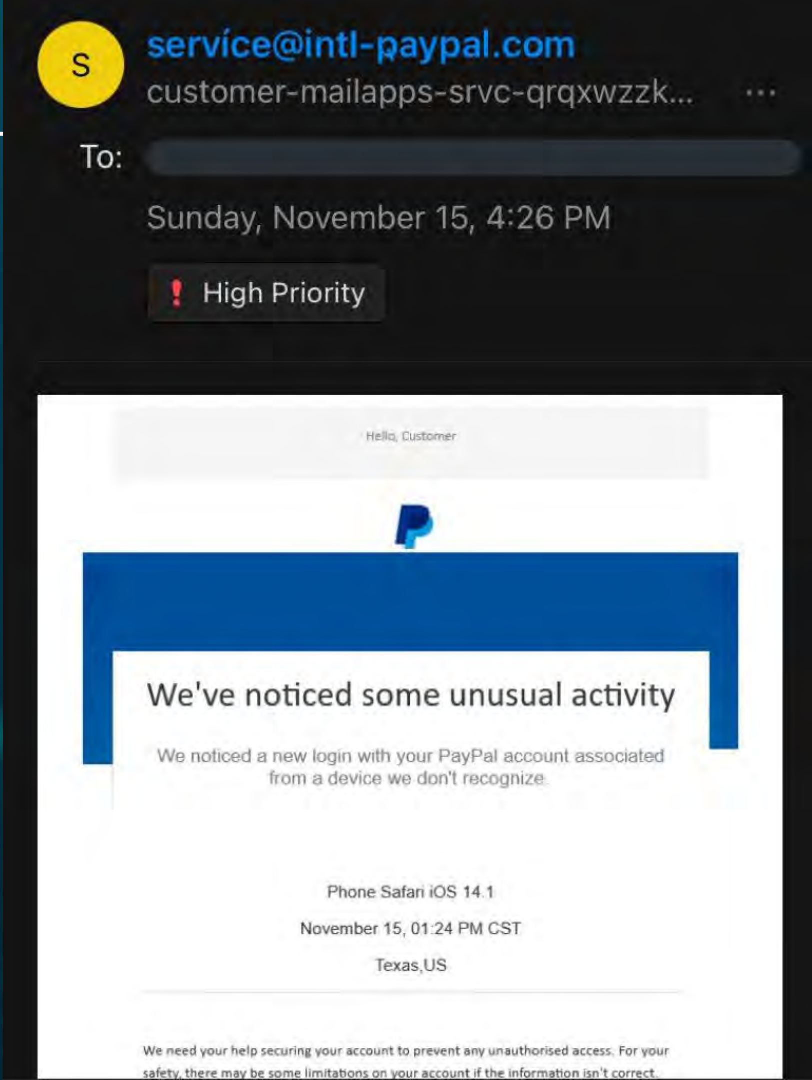
PHISHING PAGE SAMPLES

3 PHISHING EXAMPLES

- **Paypal Phishing Example**

Things to Notice:

- The mail vendor
- The mail content
- The use of sentences and words



S service@intl-paypal.com

customer-mailapps-srvc-qrqxwzzk...

To: [redacted]

Sunday, November 15, 4:26 PM

! High Priority

Hello, Customer

We've noticed some unusual activity

We noticed a new login with your PayPal account associated from a device we don't recognize

Phone Safari iOS 14.1

November 15, 01:24 PM CST

Texas,US

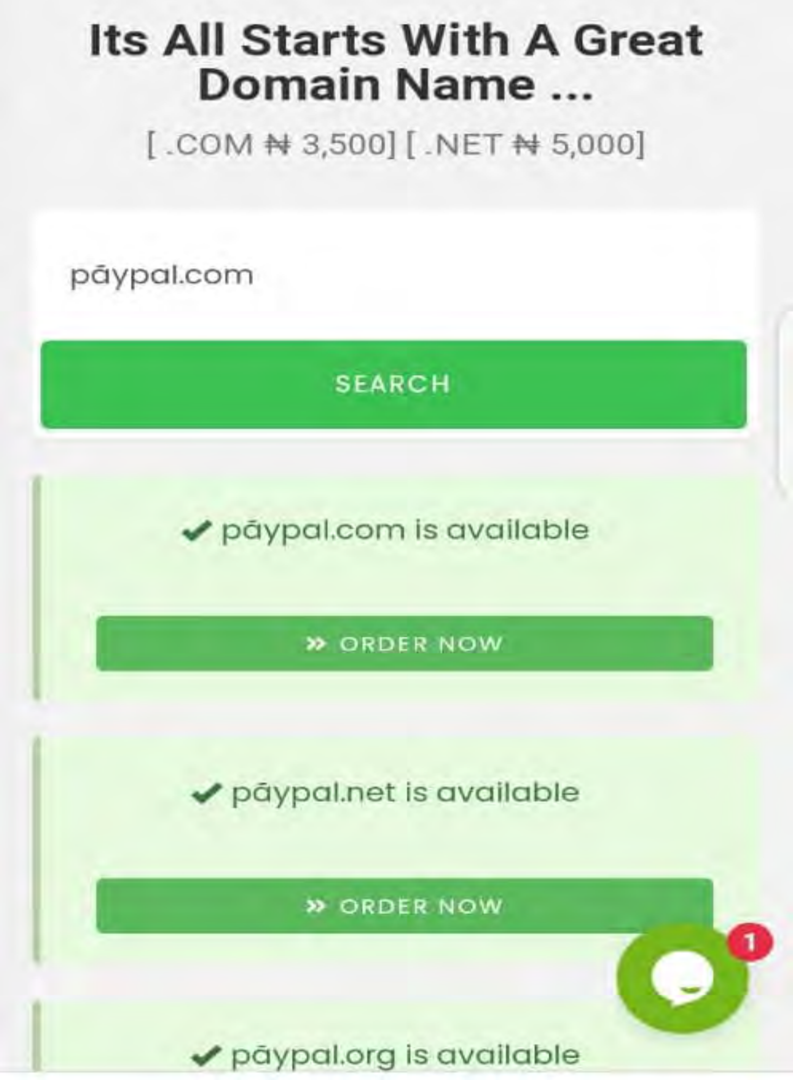
We need your help securing your account to prevent any unauthorised access. For your safety, there may be some limitations on your account if the information isn't correct.

3 PHISHING EXAMPLES

- **Paypal Phishing Example**

Things to Notice:

- Diffrent domains can be bought
- e.g .com, .com.ng, .org, e.t.c
- Long, shorthand, and german
- characters can be used
- These are cheap and available
- for free.



Its All Starts With A Great Domain Name ...

[.COM ₦ 3,500] [.NET ₦ 5,000]

päypal.com

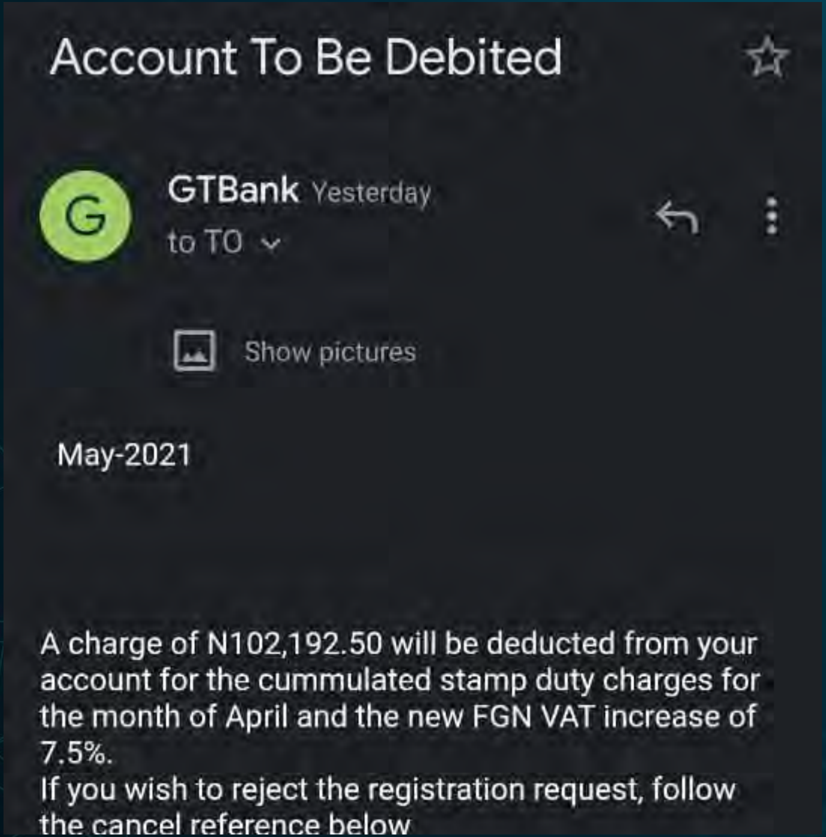
✔ päypal.com is available

✔ päypal.net is available

✔ päypal.org is available

3

EMAIL SCAM EXAMPLES



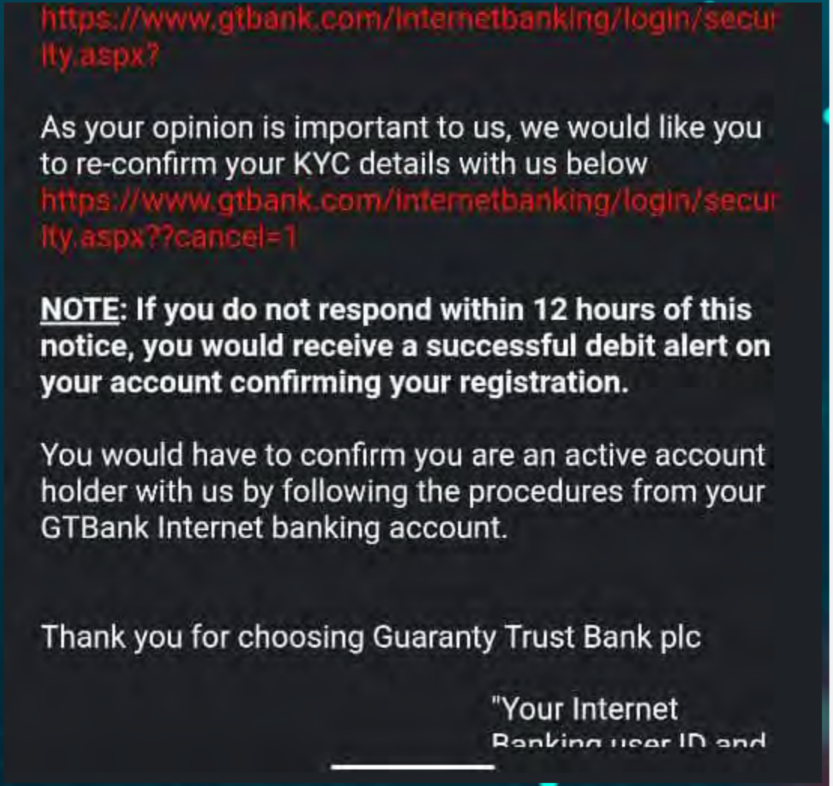
Account To Be Debited

GTBank Yesterday

to TO

May-2021

A charge of N102,192.50 will be deducted from your account for the cummulated stamp duty charges for the month of April and the new FGN VAT increase of 7.5%.
If you wish to reject the registration request, follow the cancel reference below



https://www.gtbank.com/internetbanking/login/security.aspx?

As your opinion is important to us, we would like you to re-confirm your KYC details with us below
https://www.gtbank.com/internetbanking/login/security.aspx??cancel=1

NOTE: If you do not respond within 12 hours of this notice, you would receive a successful debit alert on your account confirming your registration.

You would have to confirm you are an active account holder with us by following the procedures from your GTBank Internet banking account.

Thank you for choosing Guaranty Trust Bank plc

"Your Internet
Banking user ID and

IS MY LINK SAFE?

1 PASSWORD SECURITY

PLATFORMS TO CONFIRM IF A LINK IS SAFE

- Virustotal (analyze files & URLs to detect types of malware)
- urlvoid.com
- https://safeweb.norton.com/
- https://scanurl.net/
- https://www.phishtank.com/ (Phishing link checker)
- https://www.psafe.com/dfndr-lab/
- https://transparencyreport.google.com/safe-browsing/search

“the results are captured by Google's web crawlers and inform you if the site can be trusted.”

PASSWORD SECURITY

...

1 PASSWORD SECURITY

1. Do not use the same password, security question and answer for multiple important accounts.

2. Do not use the names of your families, friends or pets in your passwords.

3. Do not use street names, phone numbers, birthdates and so on in your passwords.

4. Do not use any dictionary word in your passwords

5. Do not use two or more similar passwords which most of their characters are same.

7. Do not let your Web browsers to store your passwords.

8. Do not log in to important accounts on the computers of others.

1 PASSWORD SECURITY

QUALITIES OF A STRONG GENERATED PASSWORD

- at least 15 characters
- uppercase letters
- lowercase letters
- numbers
- symbols, such as

` ! ” ? $? % ^ & * ( ) _ – + = { [}] : ; @ ‘ ~ # | \ < , > . ? /

1 PASSWORD SECURITY

PATTERN FOR CREATING ENCRYPTED PASSWORDS

1. Pick a name e.g “CyberSecurity”

2. Level 1 Encryption (following rules)

”Cyb3r_$3curi7y” E=3, S=$, T=7,

3. Level 2 Encryption with (rot5)

OUTPUT : “Hdg3w_$3hzwn7d”

1 PASSWORD SECURITY

Check Password Strength and validation

> https://www.my1login.com/resources/password-strength-test/
> https://password.kaspersky.com/

”CyberSecurity”	{Weak}	{Time to crack your password: 3.61 minutes}
”Cyb3r_$3curi7y”	{Medium}	{Time to crack your password: 17 hours}
” Hdg3w_$3hzwn7d”	{Very Strong}	{Time to crack your password: 44 trillion years}

Some Online Password Generators and Managers

1. https://www.dashlane.com/features/password-generator
2. https://strongpasswordgenerator.com/

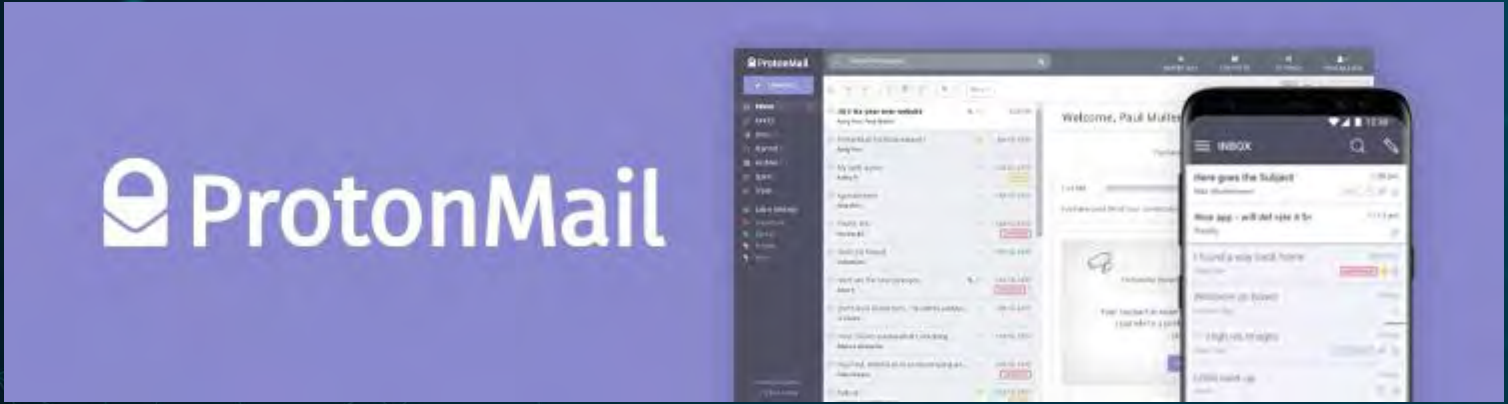
Tell yourself this ..

I will not use the same password for everything
I will not use the same password for everything
I will not use the same password for everything
I will not use the same password for everything
I will not use the same password for everything
I will not use the same password for everything
I will not use the same password for everything
I will not use the same password for everything
I will not use the same password for everything
I will not use the same password for everything
I will not use the same password for everything

TOP 5
SECURE MAIL
PROVIDERS

2 Email Security

1. ProtonMail - best ratio between price and privacy



Pros

No-logs policy

Encrypted messages to anyone

CSV contact import

Self-destructing emails

Over 20 account languages

2 **Email Security**

2. CounterMail - strongest security features

Pros

Anonymous payment

Security-first

RAM-only servers

MITM-attack protection

Safebox storage

2 Email Security

3. Tutanota - Best secure email for any device

Pros

Cheap

No-logs policy

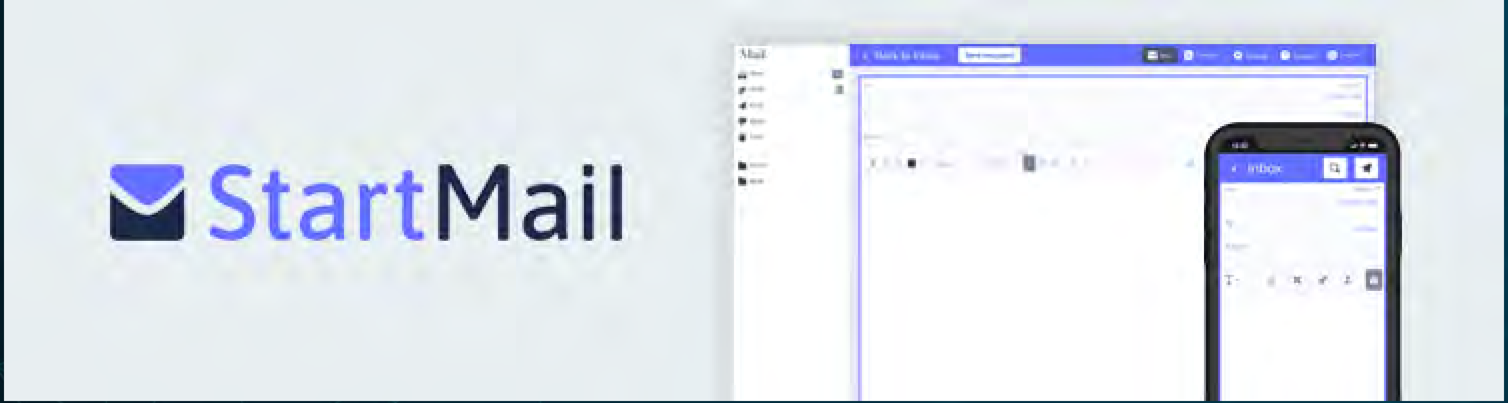
Spam filter

20+ supported languages

Encrypted calendar

2 **Email Security**

4. Startmail – best email for desktop-only users



Pros

Supports PGP

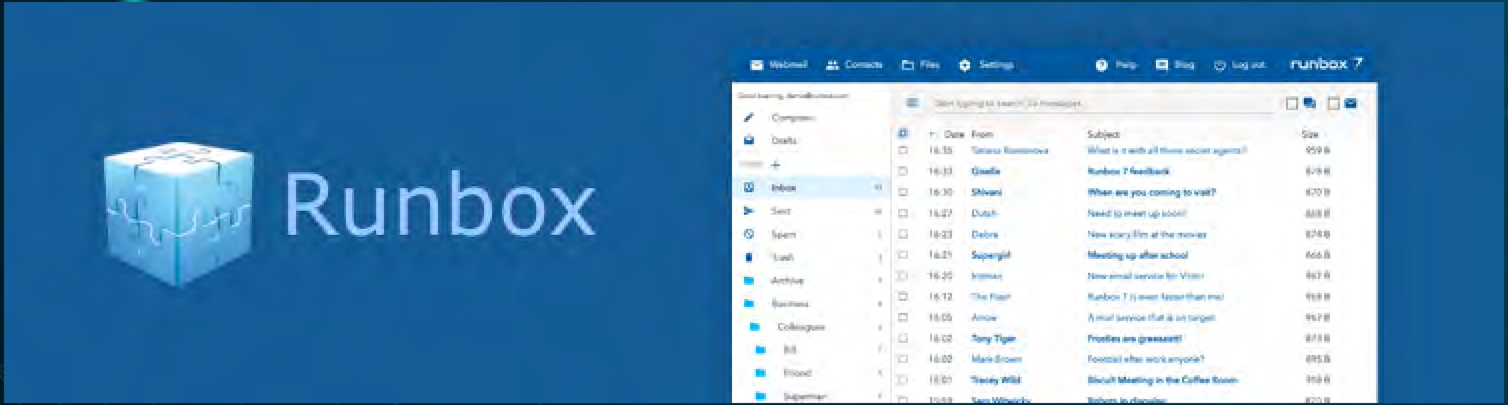
Can add multiple aliases

IMAP/SMTP support

10 GB of encrypted cloud storage

2 **Email Security**

5. Runbox – private email service with a lot of quality of life features



Date	From	Subject	Size
16:35	Tatiana Romanova	What is it with all these secret agents?	959 B
16:33	Giselle	Runbox 7 feedback	679 B
16:30	Shivani	When are you coming to visit?	670 B
16:27	Dutch	Need to meet up soon!	[illegible]
16:23	Delore	New scary film at the movies	674 B
16:21	Supergirl	Meeting up after school	666 B
16:20	Ironman	New email service for Vision	967 B
16:12	The Flash	Runbox 7 is even faster than me!	958 B
16:05	Arrow	A mail service that is on target	967 B
16:02	Tony Tiger	Profiles are grreeeat!	873 B
16:02	Mark Brown	Football after work anyone?	895 B
16:01	Tracey Wild	Biscuit Meeting in the Coffee Room	958 B
15:59	Sam Witwicky	Robots in disguise	[illegible]

Pros

Accepts cryptocurrencies

SMTP/POP/IMAP support

No ads

Intuitive UI

2 **Email Security**

WHAT TO DO IF YOUR EMAIL IS HACKED ?

1. Run a Quick Recovery check
2. Check your recent email activity to see if anything was sent that you were not aware of
3. Change your password
4. Commit to Multi Factor Authentication
5. Use different passwords for every account
6. Start using a password manager to generate random, complex passwords
7. Update your system to the latest OS and update your security software
8. Change Your Security Question
9. Run your antivirus and malware detection programs

For further protection from email hacks, it's advisable to make use of temporary mails for online registration and otp confirmation on unimportant or non trusted sites and form fills.

2 **Email Security**

Temporary Mails - No Login Required

http://www.20minutemail.com/
https://burnermail.io/
http://www.yopmail.com/en/
https://tempmailo.com/
https://www.guerrillamail.com/
https://getnada.com/
http://temp-mail.org/
https://maildrop.cc/
http://www.e4ward.com/
http://www.throwawaymail.com/
https://mytemp.email/
https://tempemailco.com/

3 Mobile Security

Tips you can use to prevent your phone from being hacked:

1) Avoid sharing passwords with friends or family
2) Avoid using the same passwords for all devices and accounts.
3) Do not open links or download attachments sent in text messages and emails without checking or confirming the source.
4) Install anti-malware software on your devices.
5) Regularly check the applications installed on your phone and remove suspicious ones
6) Ensure you have your 2fa fixed for your iCloud and all online accounts.
7) Regularly update the applications and OS of your phone.
8) Avoid connecting your device to a public Network or Wi-Fi without using a VPN.
9) Avoid visiting unsecured sites

5 SUMMARY AND CONCLUSION

CONCLUSION

Security involves assessing and testing a system to discover security risks
and vulnerabilities of the system and its data.

We define assessments as the analysis and discovery of vulnerabilities without attempting to actually exploit those vulnerabilities.

We define testing as the discovery and attempted exploitation of vulnerabilities.

Security testing is often broken out, somewhat arbitrarily, according to either the type of vulnerability being tested or the type of testing being done. A common breakout is:

- **Vulnerability Assessmen**t – The system is scanned and analyzed for security issues.
- **Penetration Testing** – The system undergoes analysis and attack from simulated malicious attackers.
- **Runtime Testing** – The system undergoes analysis and security testing from an end-user.
- **Code Review** – The system code undergoes a detailed review and analysis looking specifically for security vulnerabilities

THANKS!

Do you have any questions?