BUZZ CHRONICLES > INTERNET
Saved by @SteveeRogerr
See On Twitter

Twitter Thread by Madhu Menon

Madhu Menon
@madmanweb

The Internet and mobile phones have taken over our lives. But it comes with increasing security concerns. Website data breaches, phishing attacks, and other online scams are commonplace. Here's a thread for regular people on how to increase your security online.
#StaySafeOnline

#1
Go to your Google account settings. Revoke permissions from all the apps you don't use: https://t.co/cMGgSgtRTI

Also check if any app has access to your contacts or - gasp! - your entire email. Strongly reconsider both, especially access to your email.

Giving access to your contacts lets companies spam those people.

Giving access to your email - email organising apps, for instance - renders your online security meaningless. Password resets are often done with email, and if an external entity can access that, game over!

#2
Go to your Twitter account settings and revoke permissions from all the apps you don't use or trust:
https://t.co/lXxCgdnaXH

Online quizzes and such sites often ask for permission to post tweets for you, read your tweets, and even your DMs!.

People click "OK" without reading the fine print.

But imagine the security and privacy risk with having some unknown entity be able to post tweets and read your private DMs just to post the results of what Game of Thrones character you are.

#3
Go to your Facebook account settings and revoke permissions for all the apps you don't use: https://t.co/diMrp9pZT9

Same reason as for Twitter, but with the added risk that apps have access to vastly more data.

You might find some app there from 5+ years ago that you forgot about. Remember the Cambridge Analytica scandal? They gained access to lots of data using Facebook quizzes. People gave access to their profiles so they could post answers to dumb quizzes.

In the future, deny access to apps that want to post on social media for you or want access to your contacts. Read the permissions prompts carefully.

NEVER give access to read your email to any app.

(If you know what you're doing, that's fine. But this thread is not for you.)

#4
Always use a password manager to generate random passwords and save them.

Do NOT use the same password for all websites.

Do not use the same password with minor changes like one character modified or different number added.

Why?
The long version (do read) is here: https://t.co/HyCN0bo5el

Short version: websites store your passwords, some securely, some less so. Websites also get breached and user data gets leaked. That's the inescapable nature of technology.

If you use the same password for SiteA as for SiteB, and SiteA gets hacked, your password is now compromised. Somebody could log into SiteB with those credentials.

Random passwords ensure nobody can guess it from your personal info.
YsK!4kTu4&$yz8Bz%oq beats John29021980

Which password manager to use?
I use @BitWarden
While it lacks design polish, it's free and open source. Has a generator for creating passwords with a shortcut key (I wish I could change it from Ctrl-Shift-9 though.)

Other options:
KeePassXC
1Password
LastPass

#5
Don't rely on passwords alone. Whenever possible, enable two-factor authentication (2FA) for every major site like mail, banking, e-commerce, social media, etc. that you use.

This site keeps a list of sites that have 2FA: https://t.co/ljyS9EDpUU

Long version of what 2FA is and why you need it: https://t.co/ENA11YEeh8

Short version: it provides extra security in case your password is compromised because somebody guessed it, you wrote it down, or it was found in a data breach of another website.

I use @Authy for 2FA.

Other options:
Google Authenticator
Microsoft Authenticator

TOTP (Time-Based One-time Password) apps work even without an Internet connection. They generate number codes that are valid for a very short time. Google "how does TOTP work" for fun details.

We digress for a rant: most Indian websites only offer SMS for 2FA. SMS is insecure: it's plain text, unencrypted, passes through mobile providers and is vulnerable to SIM swap fraud (google that).
Our websites don't even offer an option for another method like a TOTP app.

#6
Some sites have "security questions" for verifying accounts. Make sure this isn't info visible on your social media pages.

"What is your favourite dish?" is not secure if you have a public FB post about how much you love mutton biryani.

#7
Go check if your account has been compromised in a data breach at https://t.co/cLbIj8FAeU

Register on the site for alerts so you know when a website has leaked your information, and possibly not disclosed it to you like they should have. (Most Indian websites have not.)

#8
When installing programs on Windows, make sure they're from a verified safe source and don't install toolbars or adware. Once an untrusted program is installed on your computer, it could log your keystrokes and it's game over!

Don't torrent cracked apps and games.

#9
Download a malware scanner like Malwarebytes (it's free) and make sure your system is clean. https://t.co/gtow8XGcPd

(Their pop-ups to upgrade are damn annoying, but the program is solid.)

Get rid of all the shit you find.

#10
No matter how much you love or trust your family / partner, don't share accounts or login info with them. You are multiplying the security risks.

Cliché: chain, weakest link, etc. All the security tips in this thread are pointless if you have access routes you don't control.

(Google has something called the Inactive Account Manager which allows you to grant access to your account to a trusted person after X days of account inactivity.)
https://t.co/jI2qqeqhhS

Useful for worst-case scenarios. ■■

Now for some mobile security tips.

Everyone has a mobile phone now, and security is often enforced through mobiles. Unfortunately, they can be stolen (easier than computers) or compromised if you don't change OS defaults. So let's go.

#10
Make sure your smartphone has auto screen lock enabled after 1-2 minutes of inactivity and needs a password to re-enable.
Number and pattern passwords are better than fingerprints and face IDs.

You leave fingerprints all over the place, remember?
And people do shit like this: https://t.co/ZIJpCwQE5u

(Oh hello, Aadhaar mafia!)

Google "fingerprint cloning" and be worried.

#11
OTPs sent to mobiles are pointless if other people can see them.

Disable displaying SMS and other messages preview on the lock screen. Or you risk a thief seeing your OTP even if your screen is locked.

How?
Android: https://t.co/wZ1dBkL8Pk
iOS: https://t.co/KJ6KyOw0aY

#12
For an additional layer of security, enable security verification for key apps like email, social media, and banking.
On Android, you can lock apps using AppLock (download).
OnePlus phones have it built-in.
iOS: https://t.co/TeyjnGVUZy

Most password reset methods use links sent to your email account. That's why I keep harping on how important it is to secure your email. Prevent casual access. Lock your phone's email app.

Your long random password is useless if they can access your email to reset it.

#13
Be wary of giving liberal permissions to apps, especially for location, storage access, and access to photos and media. Do you want your naughty photos to be visible to every app with access to your media?

Check what permissions your apps have: https://t.co/XRPrw2XlT8

Now let's talk about phishing and social engineering attacks.

These attacks are likely to be far more successful than automated hacking attempts because they prey on human psychological weaknesses.

Impersonating authority figures is an old compliance trick.

Obligatory Wikipedia links:

Phishing: https://t.co/Ias04qab4K

Social engineering: https://t.co/GvQEJBYHme

Please read if you have time. Googling those terms will also give you a lot of info.

#14
Most important tip to avoid being phished: let skepticism be your default setting.

Assume calls asking for info about your credit/debit cards aren't for real. Only give this if *you* call them through a known public contact number.

#15
NEVER give OTPs and passwords on the phone, even if Jesus himself calls and asks you.

Too many people have lost money from their account via UPI scams because of this. Don't be the next.

(I'm hoping somebody like @kingslyj has written a thread on how UPI scams work.)

Scammers often impersonate people of authority to use scare tactics into making you give up OTPs for transactions they've initiated elsewhere.

Or they use your greed to make you gift/card/prize offers for which they need an OTP.

Don't fall for any of it.

#16
Another common scam: impersonating bank or government officials to make you give up personal and financial information for "verification" purposes. They can then use this information to try hacking your other accounts.

#17

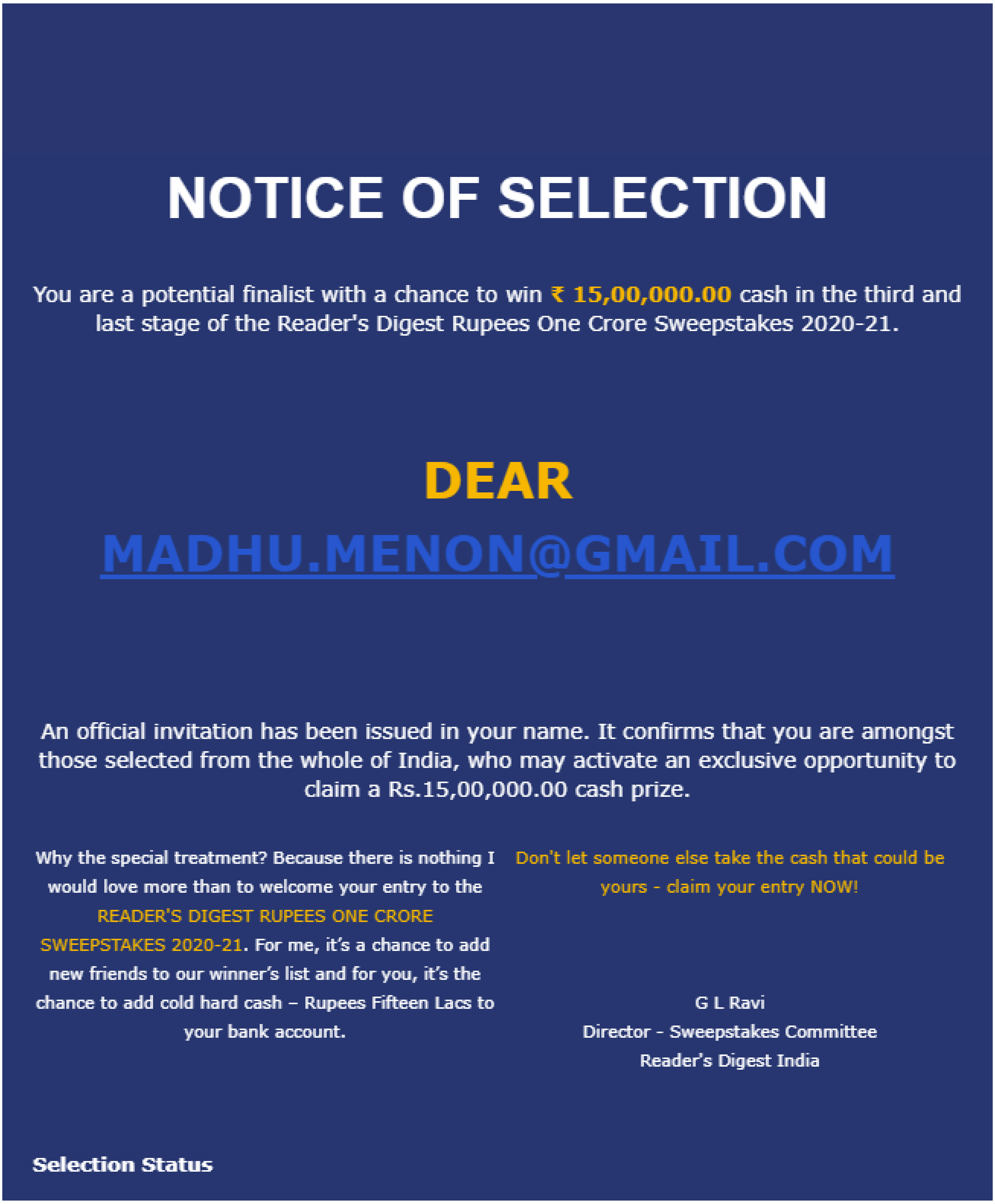
Phishing via email is an old scam. Basic mechanism: scammer pretends to be known website, scares you or tempts you into clicking a link to the website, link goes to another page designed to look like the website but exists so they can capture your username and password.

Next thing you know, your passwords have been changed and you're locked out while the scammer steals money or orders stuff from your account. Or worse, has access to your email. People get fooled because we're predisposed to trust known entities that look the part.

NEVER click on a link in an email that leads to a login form. Always type the URL directly. Scammers will set up sites like https://t.co/3NrOLymiyv that looks like https://t.co/vxOumWaaSg but have nothing to do with the original site.

Common types of sites that are impersonated: banks, educational institutions, government sites, social media platforms. Fear and greed are powerful tools.

Common tactics: "security breach, change password ASAP", "free offer", "suspicious bank transaction", "claim your prize"



NOTICE OF SELECTION

You are a potential finalist with a chance to win ₹ 15,00,000.00 cash in the third and last stage of the Reader's Digest Rupees One Crore Sweepstakes 2020-21.

DEAR MADHU.MENON@GMAIL.COM

An official invitation has been issued in your name. It confirms that you are amongst those selected from the whole of India, who may activate an exclusive opportunity to claim a Rs.15,00,000.00 cash prize.

Why the special treatment? Because there is nothing I would love more than to welcome your entry to the READER'S DIGEST RUPEES ONE CRORE SWEEPSTAKES 2020-21. For me, it's a chance to add new friends to our winner's list and for you, it's the chance to add cold hard cash – Rupees Fifteen Lacs to your bank account.

Don't let someone else take the cash that could be yours - claim your entry NOW!

G L Ravi
Director - Sweepstakes Committee
Reader's Digest India

Selection Status

Even smart and knowledgeable people can fall prey to con artists who dress up a website to look exactly like a trusted site. That's why I recommend skepticism as the default position.

Email headers too can be easily spoofed to look like they're from a legit source. These emails can then link to scam sites.

We tend to think that if something comes from a domain like https://t.co/9s3T8TDQHl, it's a legit email from https://t.co/WSipMcCA7h

Do NOT assume this.

Wrapping up, some final thoughts:

* Data protection in India is a joke. Lots of e-comm sites have had breaches. Somebody knowing stuff about you doesn't make them reliable.

* This is a thread meant for the average person to be wary, not a comprehensive security tutorial. :)

* Don't trust; verify

* More determined attackers who specifically target you (especially if you're a public figure) may have more resources to try fooling you. The more popular you are, the more cautious you should be.

* Security and convenience/usability are often trade-offs.

* Governments can probably use coercion to make entities give up info about you without your knowledge.

* Stuff you put on the Internet is only as secure as the security of the recipient or platform it's posted on. Once you send something, it's out of your hands.

This thread can be accessed by searching for "from:@madmanweb #StaySafeOnline" or bookmark this link: https://t.co/gXNqipuqyD

I will keep adding to it when I think of stuff.

Meanwhile, please RT this? And send to family and friends.

An excellent book that I recommend you all read is the classic "Influence: The Psychology of Persuasion". It's only Rs. 260 on Amazon: https://t.co/AXW2UUCEmg