Commonwealth

Best Practices to Avoid Cyber Threats

Presented by Tony DiMichele

Chief Security Awareness Officer
Commonwealth Financial Network

Hosted by
LifeTime Asset & Tax Management

801 Corporate Center Drive, Suite 110
Raleigh, NC 27607
919-845-5315

Commonwealth

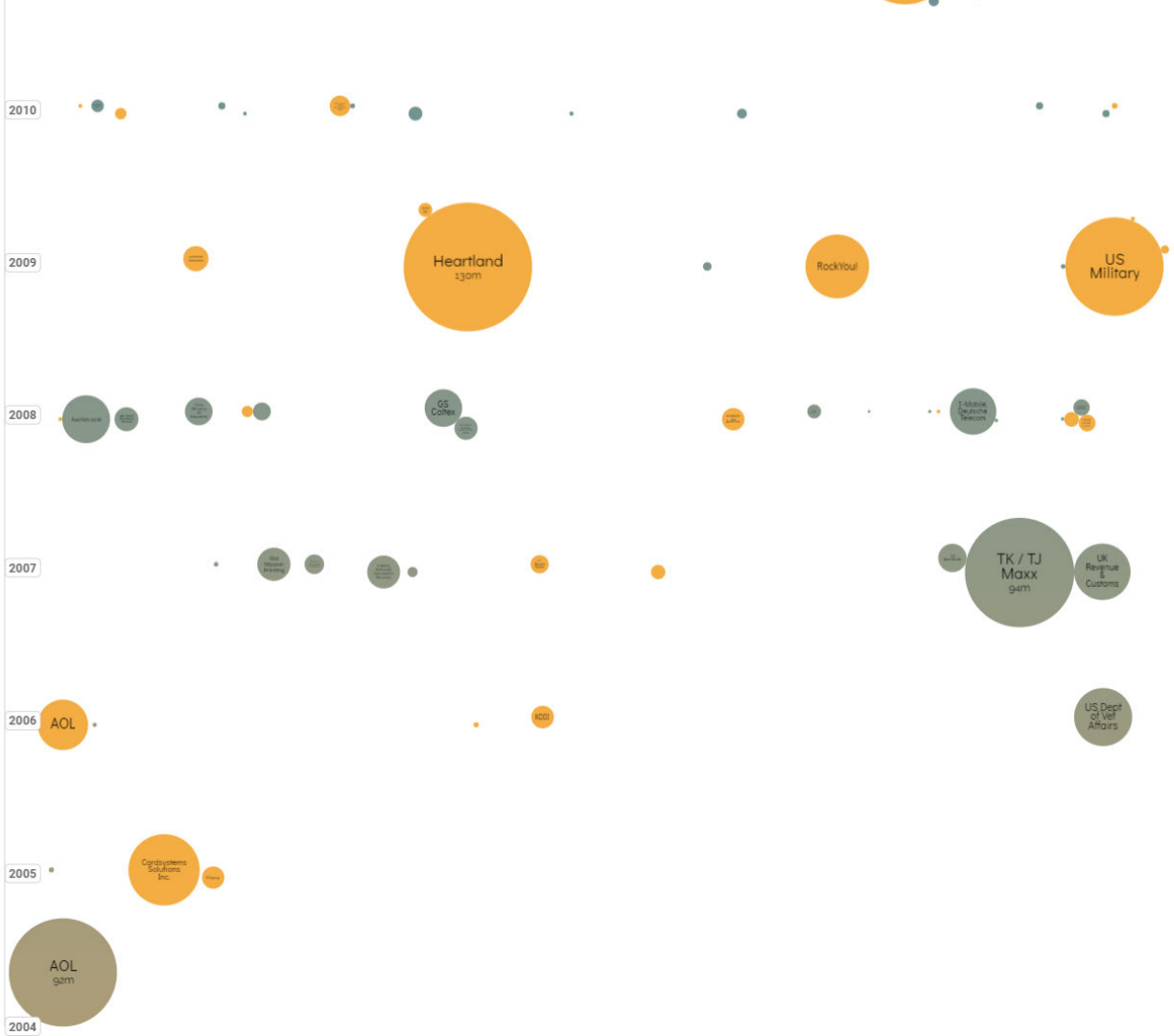
About Tony DiMichele

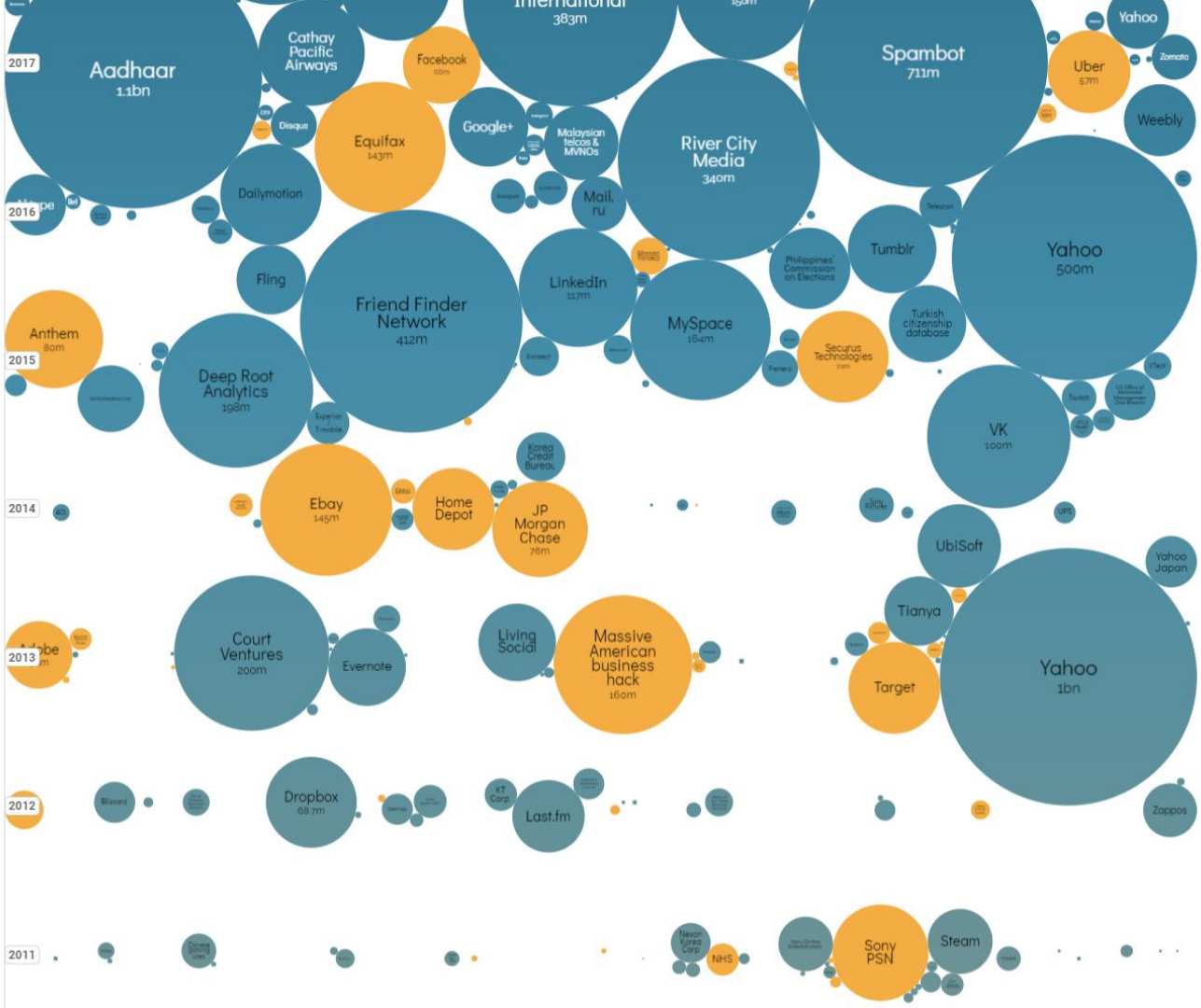
Chief Security Awareness Officer
Commonwealth Financial Network

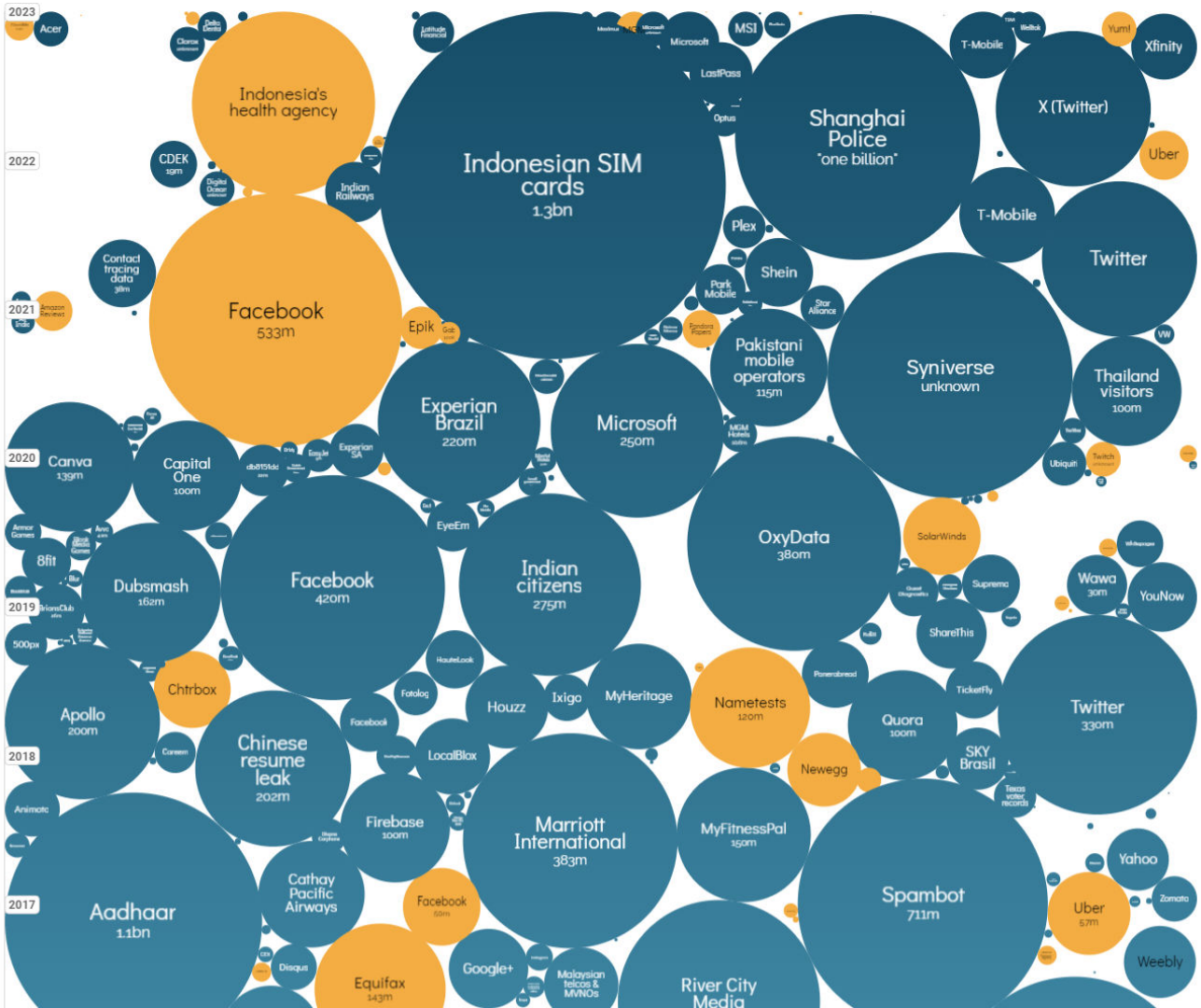
Tony and the Commonwealth team work to secure many of our technology systems, business applications, and your information against current and emerging threats.

Tony has worked with Commonwealth since 2024. He's spent over 20 years in the financial services sector where he's led enterprise information security programs and provided security consulting services.

Breach Trends


2010
2009
Heartland
130m
RockYou!
US
Military
2008
GS
Caltex
2007
TK / TJ
Maxx
94m
UK
Revenue
&
Customs
2006
AOL
US Dept
of Vet
Affairs
2005
Cardsystems
Solutions
Inc.
AOL
92m
2004

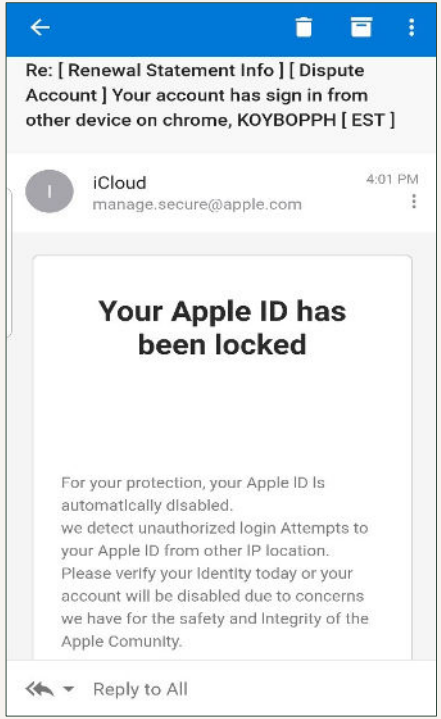

2017
2016
2015
2014
2013
2012
2011
Aadhaar
1.1bn
Cathay Pacific Airways
Facebook
60m
Disqus
Equifax
143m
Google+
Malaysian telcos & MVNOs
Dailymotion
Mail. ru
River City Media
340m
Spambot
711m
Uber
57m
Yahoo
Zomato
Weebly
Fling
Friend Finder Network
412m
LinkedIn
117m
MySpace
164m
Philippines' Commission on Elections
Tumblr
Yahoo
500m
Turkish citizenship database
Securus Technologies
Anthem
80m
Deep Root Analytics
198m
VK
100m
Ebay
145m
Home Depot
JP Morgan Chase
76m
Korea Credit Bureau
UbiSoft
Yahoo Japan
Tianya
Court Ventures
200m
Evernote
Living Social
Massive American business hack
160m
Target
Yahoo
1bn
Dropbox
68.7m
Last.fm
KT Corp
Zappos
Nexon Korea Corp
NHS
Sony PSN
Steam

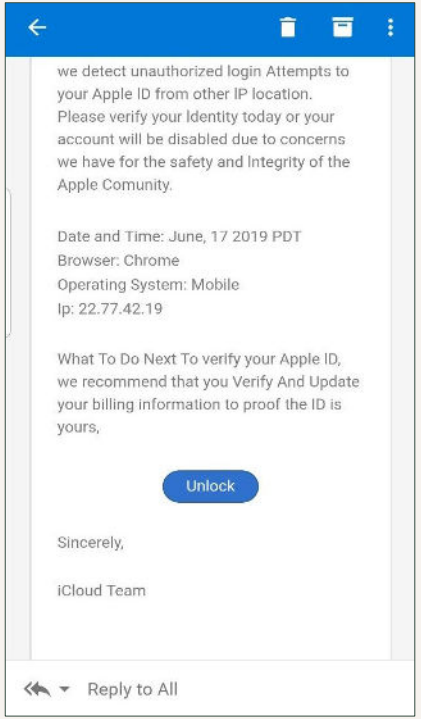

2023
2022
2021
2020
2019
2018
2017
Acer
Indonesia's health agency
Indonesian SIM cards 1.3bn
Microsoft
LastPass
MSI
Optus
Shanghai Police "one billion"
T-Mobile
Yum!
Xfinity
X (Twitter)
Uber
CDEK 19m
Indian Railways
T-Mobile
Twitter
Plex
Shein
Park Mobile
Star Alliance
Contact tracing data 3bn
Facebook 533m
Epik
Pakistani mobile operators 115m
Syniverse unknown
VW
Thailand visitors 100m
Experian Brazil 220m
Microsoft 250m
Canva 139m
Capital One 100m
Experian SA
EyeEm
Ubiquiti
Twitch
OxyData 38om
SolarWinds
Supremo
Wawa 30m
YouNow
8fit
Dubsmash 162m
Facebook 420m
Indian citizens 275m
ShareThis
Chtrbox
Apollo 200m
Chinese resume leak 202m
Houzz
Ixigo
MyHeritage
Nametests 120m
Quora 100m
TicketFly
Twitter 330m
SKY Brasil
Newegg
LocalBlox
Firebase 100m
Marriott International 383m
MyFitnessPal 150m
Spambot 711m
Yahoo
Zomato
Uber 57m
Weebly
Cathay Pacific Airways
Facebook 50m
Aadhaar 1.1bn
Disqus
Equifax 143m
Google+
Malaysian telcos & MVNOs
River City Media

Common Threats

Email Phishing Scams

In the past year, 76% of businesses reported that they had been the victim of a phishing attack.

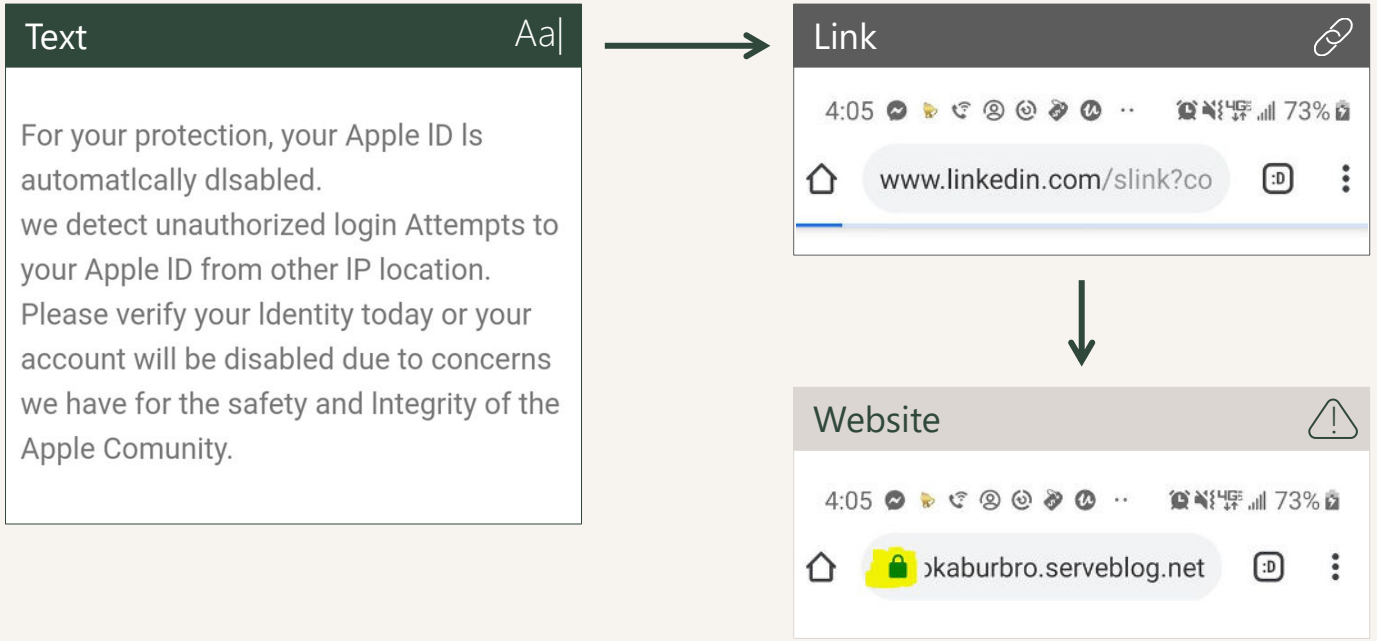




Source: Wombat

Email Phishing Scams

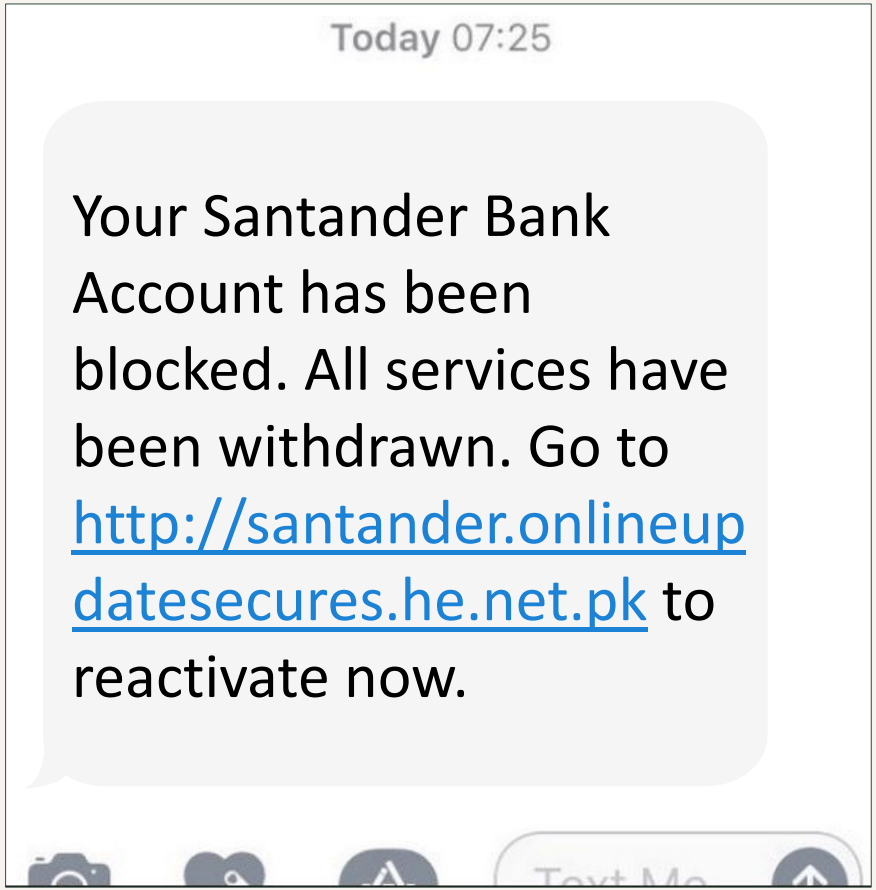
In the past year, 76% of businesses reported that they had been the victim of a phishing attack.



Source: Wombat

Phone Scams

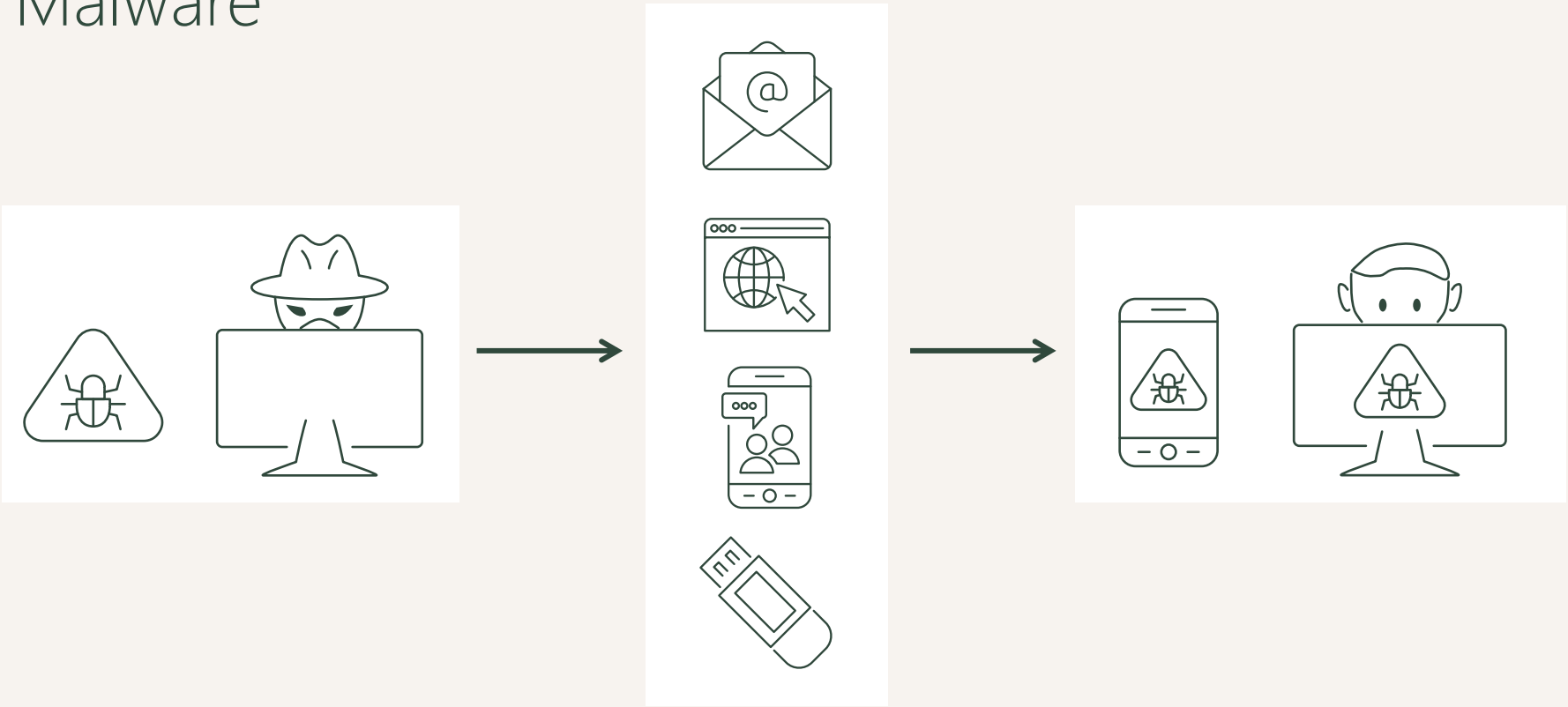
- **Vishing (voice phishing)** attacks through phone calls or voice messages
- **Smishing (SMS phishing)** attacks through text messages



Malware

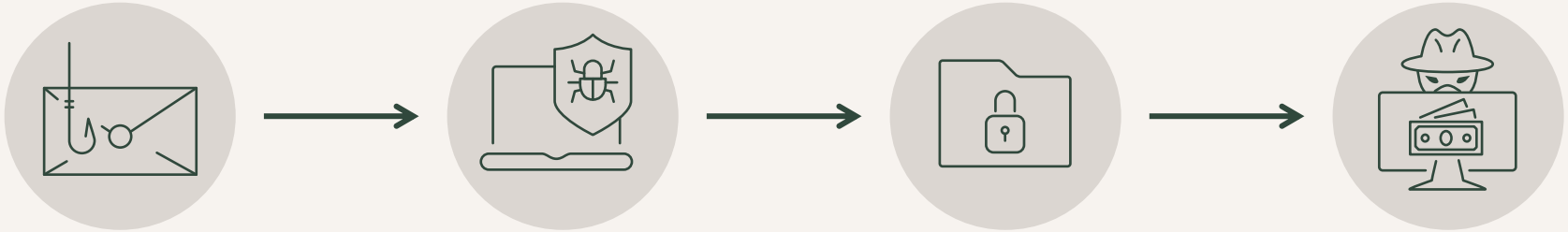

Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

Malware



Ransomware

- Criminal holds a victim's data at ransom
- Even if a ransom is paid, it is not always guaranteed the data will be returned to the victim



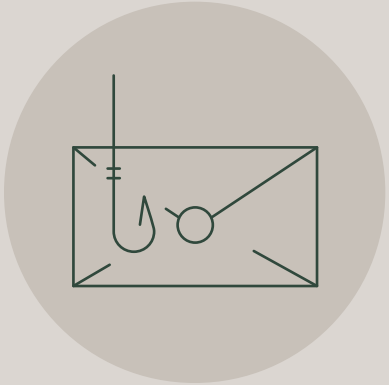
Victim receives phishing email containing malicious attachment

Malware is installed on victim's device

Victim's files are encrypted by criminal and cannot be accessed without decryption key

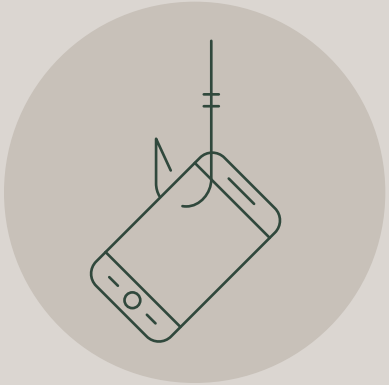
Criminal demands ransom in exchange for decryption key

Best Practices



Email Phishing Scams

- Do **not** click on unfamiliar links
- Delete the email, do **not** forward the email
- Verify with the sender through a phone number you are familiar with
- Do **not** provide sensitive information
- When in doubt . . . throw it out! Report suspicious emails through your email provider



Phone Scams

- Do **not** open links from unknown SMS text messages
- Do **not** provide sensitive information to an unknown caller
- Verify the phone number and call the institution directly

Malware Infection

- Keep your internet browser updated
- Do **not** open email attachments without verification
- Do **not** download software from untrusted sources
- Avoid using USB removable drives from untrusted sources

Strong Passwords Can Make a Difference

Passwords	Time to Crack
common	Seconds
Ge8%#B	Minutes
C0mm0nw34lth	One Day
tlpWENT2mkt.	Months-Years

Passwords

- Use long, complex passwords and passphrases.
  - I am Secure Today ➜ #IamS3cure!T0day
- Change your passwords regularly.
- **Do not** use the same password for multiple accounts.
- **Do not** use personal identifiers within your password.
- **Do not** use a full dictionary word.

Password Safety Tools

- Password managers
- Multifactor authentication (MFA)

Keeping Your Devices and Accounts Safe

Best Practices

Use strong, complex passwords and passphrases

- Minimum of 12 characters, using a combination of:
  - Upper- and lowercase letters
  - Numbers
  - Symbols (!@#$%^&*)
- Do not reuse passwords for multiple accounts

Enable multifactor authentication (MFA)

Requires you to provide two or more verification factors to gain access to a resource such as an application, online account, or VPN

Enable alerts on accounts

Get notified about suspicious activity on your accounts

- Logins from unrecognized devices
- Transactions on financial accounts
- Password and/or settings updates

Best Practices

Perform regular updates on devices and apps

- Fixes vulnerabilities that criminals attempt to exploit
- Set devices to automatically perform updates once they are available or perform updates as soon as they are available

Be wary of untrusted sources

- Verify the legitimacy of a request, before:
  - Clicking on links or opening attachments
  - Downloading software or files
- Do not provide sensitive information over the phone or email

Establish backup processes for your systems

Get notified about suspicious activity on your accounts

- Ransomware attacks
- Lost/stolen devices
- Damaged devices

Preventing Identity Theft

Create a My Social Security Account

- Visit **www.SSA.gov**
- Prevents cybercriminals from accessing your social security benefits or creating an account under your name
- Ideal for people age 65+ or those who collect benefits, but available for everyone

Freeze Your Credit

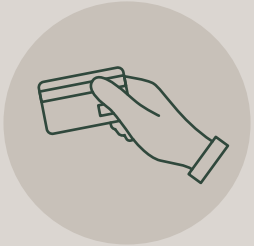
- Prevents new account fraud
- No cost – **free!**
- Must be filed individually with each credit bureau
- Quick to lift or “thaw” a frozen account if you need to apply for a new account
- Does not affect open accounts or credit scores
- Available for everyone – **even children!**

Credit Freeze Vs. No Credit Freeze

Criminal obtains victim's social security number

Criminal applies for credit cards using victim's identity

Access to victim's credit history



Criminal obtains credit card under victim's name

Credit freeze prevents new account(s) from being open

Application rejected

Lifting a Credit Freeze

You apply for an auto loan

Access to credit history

Application approved

You lift the freeze with a PIN

You freeze the report again

How to Obtain a Credit Freeze

Contact each of the 3 credit bureaus:

- **Equifax:** 800-349-9960
- **Experian:** 888-397-3742
- **TransUnion:** 888-909-8872

Credit freezes can also be placed on each of the credit bureau websites or by mail.

Protecting the Paper in Your Life

- Store documents in a secure location (i.e., lockbox, locked filing cabinet)
- Retrieve mail as quickly as possible
- Take outgoing mail directly to the post office
- Pay bills online and opt for paperless statements
- Use gel pens when writing checks
- Use a shredder before disposing

Secure Data Disposal

Documents with personal data should be disposed of properly with secure shredders:

- Social security numbers
- Birthdates
- Account numbers
- Passwords
- PINs

Secure shredders:

- Cross cut
- Diamond cut
- Micro cut

Questions?

Thank You

Tony DiMichele
adimichele@commonwealth.com