Forearmed.

Phishing Attacks and Password Cracking.

Prof. Dr. Andreas Aßmuth

Technical University of Applied Sciences
OTH Amberg-Weiden

Department of Electrical Engineering, Media and
Computer Science

2021-05-29

About me

Professor of Computer Networks and Mathematics

Dean of Studies

Teaching:

Mathematics, Computer Networks, Cryptography, Coding Theory, Information Security

Research:

Applied Cryptography, Information Security, Ethical Hacking

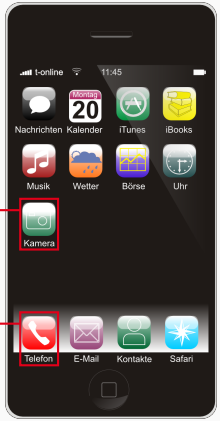
IARIA Fellow

Anatomy of a Hacked Smartphone

Anatomy of a Hacked Smartphone

Surveillance

- ☞ Audio
- ☞ Camera
- ☞ Call logs
- ☞ Position
- ☞ SMS

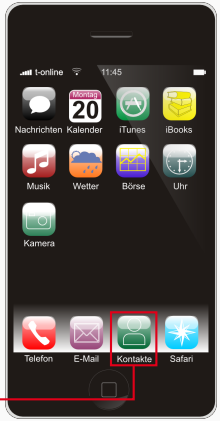


Anatomy of a Hacked Smartphone

Surveillance

Data Theft

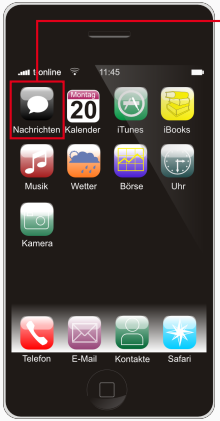
- ☞ Account infos
- ☞ Contacts
- ☞ Call logs
- ☞ Theft through apps
- ☞ Device infos (IMEI)



Anatomy of a Hacked Smartphone

Surveillance

Data Theft



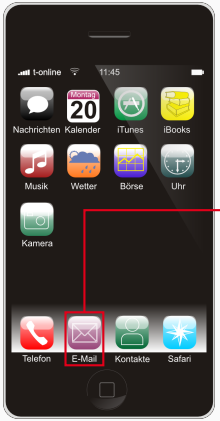
Money

- ☞ Premium SMS
- ☞ Theft of TANs
- ☞ Ransomware
- ☞ Fake Antivirus
- ☞ Overpriced calls

Anatomy of a Hacked Smartphone

Surveillance

Data Theft



Money

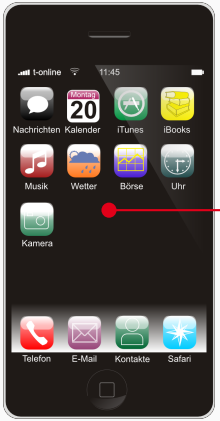
Faked Identity

- ☞ Re-routing of SMS
- ☞ Sending emails
- ☞ Posts on social media

Anatomy of a Hacked Smartphone

Surveillance

Data Theft



Money

Faked Identity

“Zombie Smartphone”

- ☞ DDoS attacks
- ☞ Clickbait

Cryptographic Hash Functions

Cryptographic hash functions must have certain **properties**:

(i) Fast and easy computation of hashes.

Cryptographic Hash Functions

Cryptographic hash functions must have certain **properties**:

(i) Fast and easy computation of hashes.

(ii) One-way function: Given a hash, it must be infeasible to find an input that generates exactly that hash.

Cryptographic Hash Functions

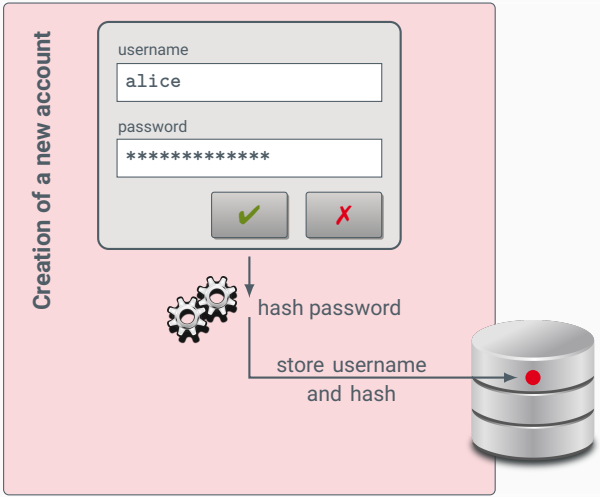
Cryptographic hash functions must have certain **properties**:

(i) Fast and easy computation of hashes.

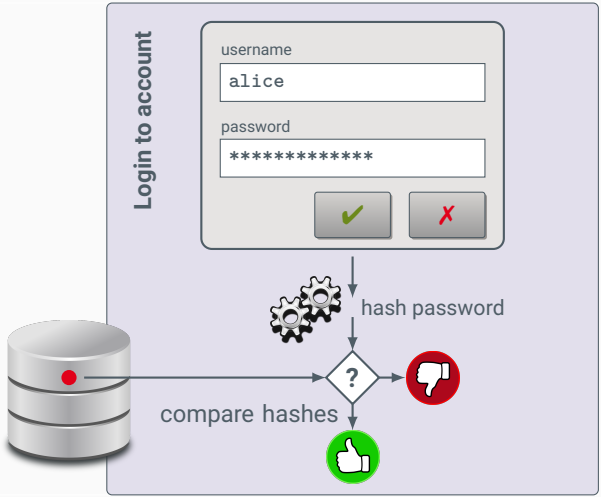
(ii) One-way function: Given a hash, it must be infeasible to find an input that generates exactly that hash.

(iii) Collision resistance: It must not be possible to find any two inputs that generate the same hash.

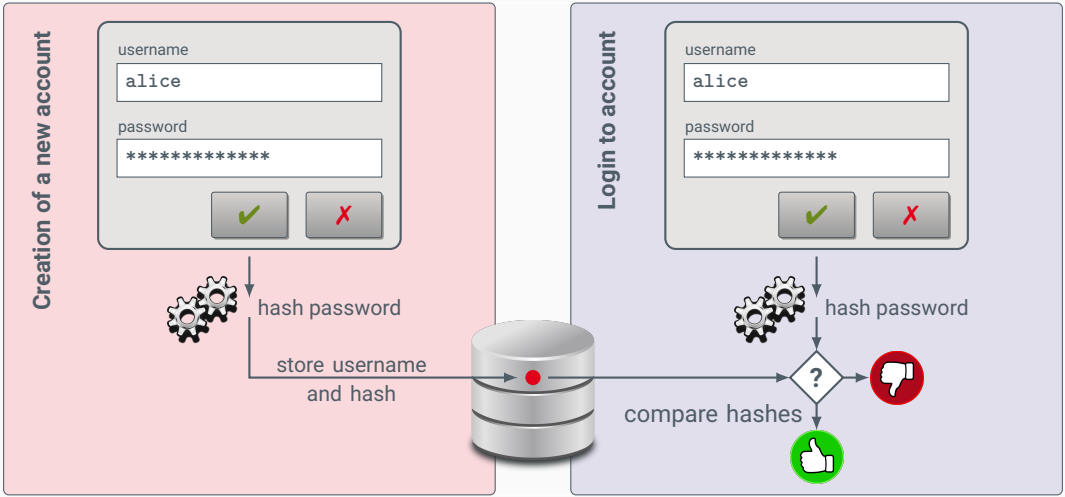
How Does a Login Procedure Work?



How Does a Login Procedure Work?



How Does a Login Procedure Work?

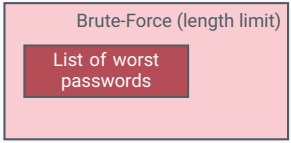


Password Cracking Offline Attack

List of worst passwords

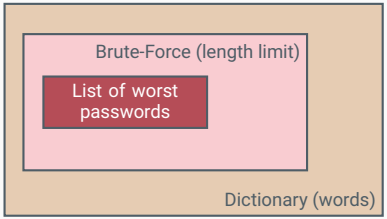
Cf. Javier Galbally, Iwen Coisel and Ignacio Sanchez, “A New Multimodal Approach for Password Strength Estimation—Part I: Theory and Algorithms”, IEEE Trans. on Information Forensics and Security, Vol. 12, No. 12, pp. 2829-2844, doi: 10.1109/TIFS.2016.2636092, IEEE, 2017.

Password Cracking Offline Attack



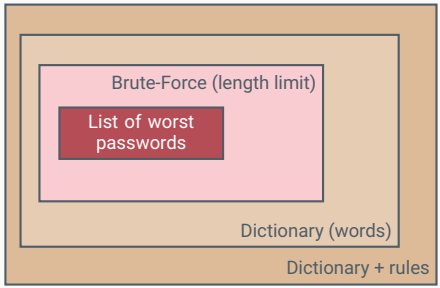
Cf. Javier Galbally, Iwen Coisel and Ignacio Sanchez, "A New Multimodal Approach for Password Strength Estimation—Part I: Theory and Algorithms", IEEE Trans. on Information Forensics and Security, Vol. 12, No. 12, pp. 2829-2844, doi: 10.1109/TIFS.2016.2636092, IEEE, 2017.

Password Cracking Offline Attack



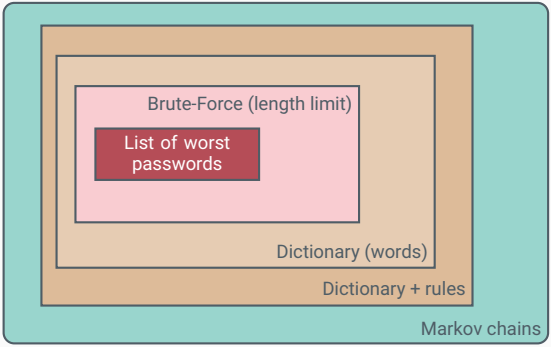
Cf. Javier Galbally, Iwen Coisel and Ignacio Sanchez, "A New Multimodal Approach for Password Strength Estimation—Part I: Theory and Algorithms", IEEE Trans. on Information Forensics and Security, Vol. 12, No. 12, pp. 2829-2844, doi: 10.1109/TIFS.2016.2636092, IEEE, 2017.

Password Cracking Offline Attack



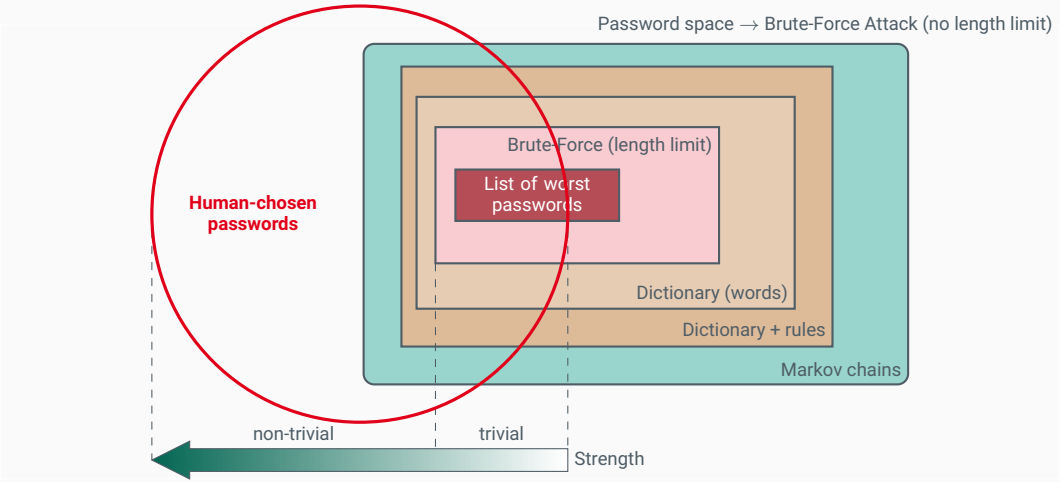
Cf. Javier Galbally, Iwen Coisel and Ignacio Sanchez, "A New Multimodal Approach for Password Strength Estimation—Part I: Theory and Algorithms", IEEE Trans. on Information Forensics and Security, Vol. 12, No. 12, pp. 2829-2844, doi: 10.1109/TIFS.2016.2636092, IEEE, 2017.

Password Cracking Offline Attack



Cf. Javier Galbally, Iwen Coisel and Ignacio Sanchez, "A New Multimodal Approach for Password Strength Estimation—Part I: Theory and Algorithms", IEEE Trans. on Information Forensics and Security, Vol. 12, No. 12, pp. 2829-2844, doi: 10.1109/TIFS.2016.2636092, IEEE, 2017.

Password Cracking Offline Attack



Cf. Javier Galbally, Iwen Coisel and Ignacio Sanchez, "A New Multimodal Approach for Password Strength Estimation—Part I: Theory and Algorithms", IEEE Trans. on Information Forensics and Security, Vol. 12, No. 12, pp. 2829-2844, doi: 10.1109/TIFS.2016.2636092, IEEE, 2017.

Grapucino Graphic Processing Unit Cluster in a Box

Figure created by Tobias Nickl, M.Sc.

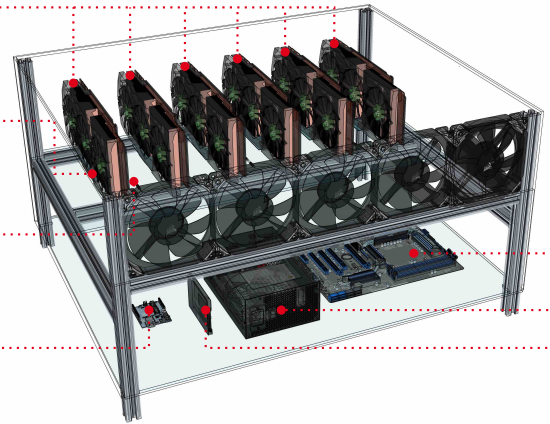
Grapucino Graphic Processing Unit Cluster in a Box

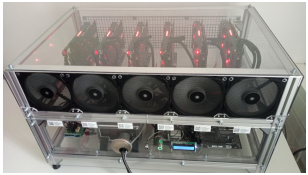
Graphics Cards
GeForce GTX 1080

Riser Adapter Boards
1x → 16x

Temperature Sensors

Fan Control
Arduino Uno





Power Supply
1600 W

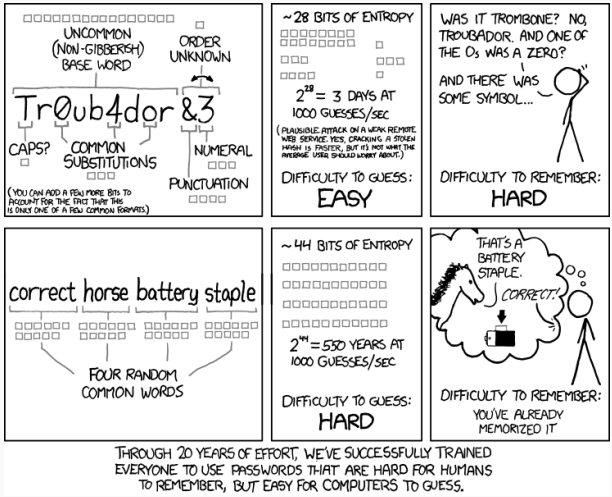
256 GB SSD

Figure created by Tobias Nickl, M.Sc.

Password Cracking

Demonstration

Secure Passwords Summary



Source: Randall Munroe, https://xkcd.com/936/

Phishing Example 1

Von Amazon Kundensupport <info@clientsupportpanel.org>
Betreff **Ihre Bestellung wurde storniert!**
An a.assmuth@haw-aw.de

amazon.de

Meine Bestellung | Mein Konto | Amazon.de

Bestellung storniert

Referenz: #471-1086479-5478260

Guten Tag,

aufgrund diverser Widrigkeiten wärend des Bestellablaufs, wurde Ihr Nutzerkonto zum Schutz vorsorglich gesperrt. Womöglich erfolgte ein unberechtigter Zugang auf Ihr Konto.

Bitte bestätigen Sie sich als primärer Kontoinhaber, um eine erneute Wiederaufnahme der Handlungsfähigkeit des Kontos zu realisieren.

Folgen Sie dazu bitte den Hinweisen am Ende dieser Benachrichtigung.

Zustellung:

Dienstag, 5. September 2017 - Mittwoch, 6. September 2017

Versandart:
Standardversand

Die Bestellung geht an:

Radoslav Sapisacut
Packstation 121
Arnulf-Klett-Platz 2
Stuttgart, Baden-Württemberg
70173
Deutschland

Einzelheiten Ihrer Bestellung

Bestellung: #471-1086479-5478260
Aufgegeben am 3. September 2017

Apple iPhone 7 Smartphone (11,9 cm (4,7 Zoll), 128GB interner Speicher, iOS 10) matt schwarz — **EUR 729,00**
Zustand: Neu
Verkauft von: Amazon EU S.a.r.L.

Zwischensumme:	EUR 590,49
Verpackung und Versand:	EUR 0,00
Zwischensumme ohne USt.:	EUR 590,49
Umsatzsteuer:	EUR 138,51
Endbetrag inkl. USt.:	**EUR 729,00**

Die Wiederherstellung der uneingeschränkten Handlungsfähigkeit Ihres Kundenkontos, erfolgt unverzüglich nach erfolgreichem Abschluss des Verifizierungsprozesses.

Verifizierung starten

Bitte achten Sie bei Ihren Angaben auf die korrekte Schreibweise, da eine Wiederherstellung bei erheblicher Abweichung zu den hinterlegten Daten, nur noch über den Postweg möglich ist.

Wir bedauern diese Unannehmlichkeiten,
Amazon.de

Phishing Example 1

Von Amazon Kundensupport <info@clientsupportpanel.org>
Betreff **Ihre Bestellung wurde storniert!**
An a.assmuth@haw-aw.de

amazon.de

Meine Bestellung | Mein Konto | Amazon.de

Bestellung storniert

Referenz: #471-1086479-5478260

Guten Tag,

aufgrund diverser Widrigkeiten wärend des Bestellablaufs, wurde Ihr Nutzerkonto zum Schutz vorsorglich gesperrt. Womöglich erfolgte ein unberechtigter Zugang auf Ihr Konto.

Bitte bestätigen Sie sich als primärer Kontoinhaber, um eine erneute Wiederaufnahme der Handlungsfähigkeit des Kontos zu realisieren.

Folgen Sie dazu bitte den Hinweisen am Ende dieser Benachrichtigung.

Zustellung:	Die Bestellung geht an:
Dienstag, 5. September 2017 - Mittwoch, 6. September 2017	**Radoslav Sapisacut** **Packstation 121** **Arnulf-Klett-Platz 2** **Stuttgart, Baden-Württemberg** **70173** **Deutschland**
Versandart: **Standardversand**	

Einzelheiten Ihrer Bestellung

Bestellung: #471-1086479-5478260
Aufgegeben am 3. September 2017

Apple iPhone 7 Smartphone (11,9 cm (4,7 Zoll), 128GB interner Speicher, iOS 10) matt schwarz — **EUR 729,00**
Zustand: Neu
Verkauft von: Amazon EU S.a.r.L.

Zwischensumme:	EUR 590,49
Verpackung und Versand:	EUR 0,00
Zwischensumme ohne USt.:	EUR 590,49
Umsatzsteuer:	EUR 138,51
Endbetrag inkl. USt.:	**EUR 729,00**

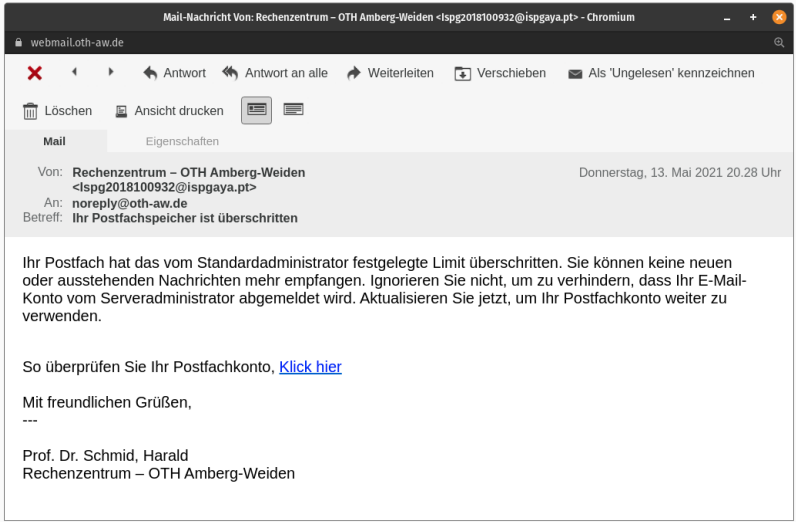
Die Wiederherstellung der uneingeschränkten Handlungsfähigkeit Ihres Kundenkontos, erfolgt unverzüglich nach erfolgreichem Abschluss des Verifizierungsprozesses.

☞ https://gglks.com/8i43k

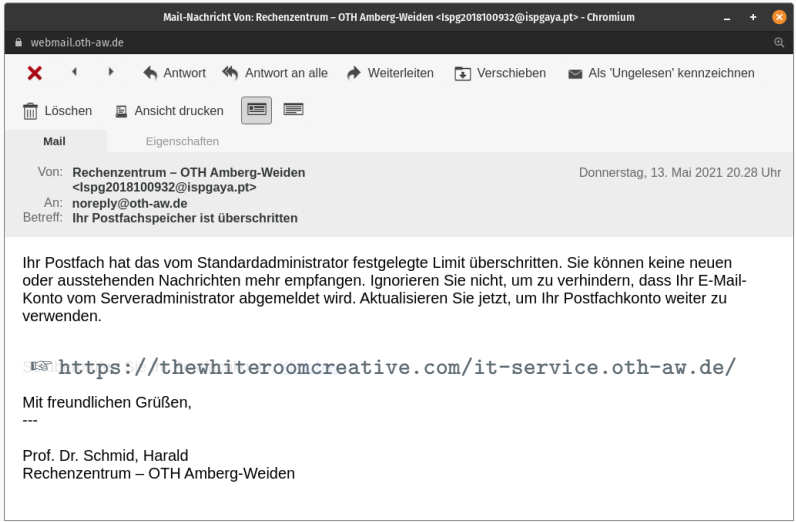
Bitte achten Sie bei Ihren Angaben auf die korrekte Schreibweise, da eine Wiederherstellung bei erheblicher Abweichung zu den hinterlegten Daten, nur noch über den Postweg möglich ist.

Wir bedauern diese Unannehmlichkeiten,
Amazon.de

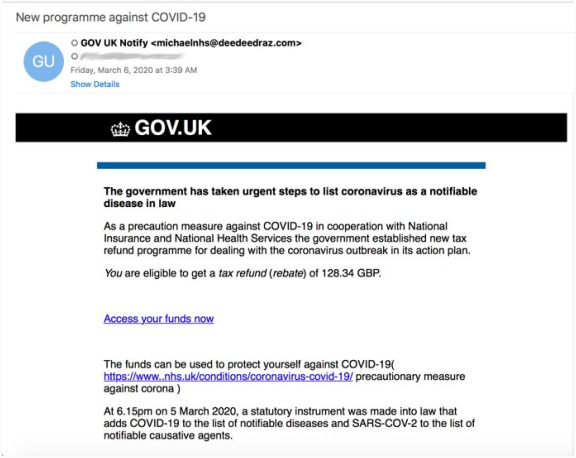
Phishing Example 2



Phishing Example 2



Phishing Example 3



New programme against COVID-19

GU

GOV UK Notify <michaelnhs@deedeedraz.com>

Friday, March 6, 2020 at 3:39 AM

Show Details

GOV.UK

The government has taken urgent steps to list coronavirus as a notifiable disease in law

As a precaution measure against COVID-19 in cooperation with National Insurance and National Health Services the government established new tax refund programme for dealing with the coronavirus outbreak in its action plan.

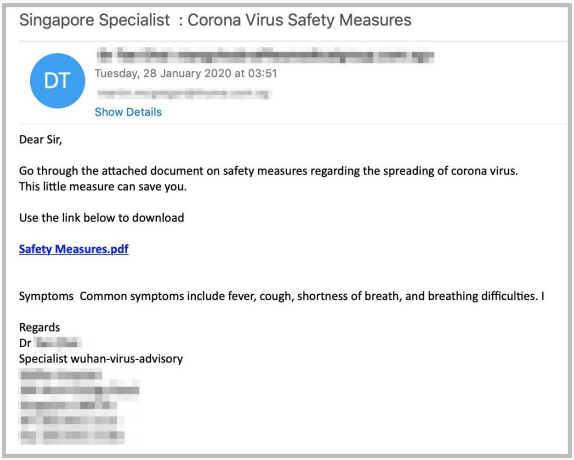
You are eligible to get a *tax refund* (*rebate*) of 128.34 GBP.

Access your funds now

The funds can be used to protect yourself against COVID-19(https://www..nhs.uk/conditions/coronavirus-covid-19/ precautionary measure against corona)

At 6.15pm on 5 March 2020, a statutory instrument was made into law that adds COVID-19 to the list of notifiable diseases and SARS-COV-2 to the list of notifiable causative agents.

Phishing Example 4



Singapore Specialist : Corona Virus Safety Measures

DT

Tuesday, 28 January 2020 at 03:51

Show Details

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.
This little measure can save you.

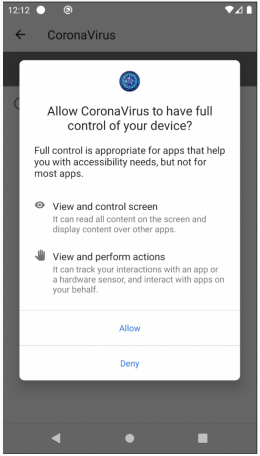
Use the link below to download

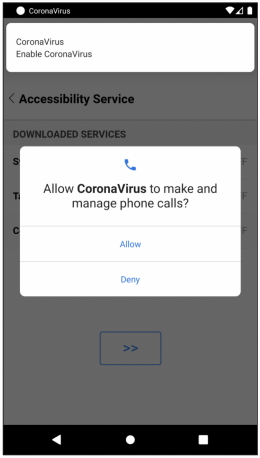
Safety Measures.pdf

Symptoms Common symptoms include fever, cough, shortness of breath, and breathing difficulties. I

Regards
Dr
Specialist wuhan-virus-advisory

Malicious COVID-19 Apps





Phishing Attack

Demonstration

Prof. Dr. Andreas Aßmuth
Professor für Rechnernetze und Mathematik

OTH Amberg-Weiden
Fakultät Elektrotechnik, Medien und Informatik

Kaiser-Wilhelm-Ring 23, 92224 Amberg
Tel.: +49 9621 482 3604
Fax: +49 9621 482 4604
Email: a.assmuth@oth-aw.de
PGP: 0x93E4 D0FA
Web: https://www.andreas-assmuth.de
https://www.oth-aw.de