

# Beginners Guide to Online Safety ! (Not only for Seniors)

presented by Uwe Dotzauer

Saturday June 18th

For the OPCUG and PATACS Joint Meeting





# Agenda

- \* Identify the Scam
- \* What can you do about it ?
  - \* Secure your Computer
- \* What to do when it happens ?
  - \* Questions ?





# TOP 10 SCAMS 2021

- Romance
- Tech Support
- Grandparent
- Government Impersonating
  - Sweepstakes
  - Home repair
  - TV / Radio
- Family Caregiver
- Zoom Phishing
- COVID 19 vaccination card scam





# Top Online Scams 2020

Rank	Scam Type	% of total
1	Internet: Gen Merchandise	41.88%
2	Phishing/Spoofing	11.20%
3	Fake Check Scams	10.06%
4	Friendship & Sweetheart Swindles	9.01%
5	Prizes/Sweepstakes/Free Gifts	5.11%
6	Advance Fee Loans, Credit Arrangers	4.25%
7	Computers: Equipment/Software	2.03%
8	Internet: Auctions	1.49%
9	Investments: Other (note in comments)	1.43%
10	Internet: Extortion Scams	1.36%







# Typical Red Flags



- ★ Promise of Money and Riches
  - ★ CAN'T meet in Person
    - ★ Pressure / ASAP
    - ★ Price too good to be true
- ★ NO CHECK OR CC (crypto or gift cards instead)
  - ★ CAN'T take your phone call
  - ★ CAN'T find them on the INTERNET
- ★ They are in LOVE with you but won't do FACETIME





# Peer to Peer Payment Scam

- Only use with friends and family only
  - ***Be suspicious if contact info changes***
- NO urgent payment request ( RUSH )
- NO payment for utilities bills etc
- Insist of using P2P
- Once you hit send....it's gone



CM  
Uwe Dotzauer  
703-340-6230



# Money Mule

- Someone who transfers or moves illegally acquired money on behalf of someone else

- Solicited via online romance scheme or “WORK from Home” job offer
- Asked to open NEW bank account
- Receive money from someone YOU never met in person
- Asked to “ wire money “ via mail, P2P, money order, etc.
- Allowed to keep portion of the money
- “ Online Date “ ask you to help her with transfer



**Only a fool is a 'money mule'** 

Criminals may ask to use your bank account to transfer or store money. If you agree you could be jailed for 'money muling'.



**#Tell2**  
Keep friends and family safe by telling two people about this campaign.

Google North Yorkshire Police  
Take Five to find out more about scams and how to avoid them or visit [www.actionfraud.police.uk](http://www.actionfraud.police.uk)

Don't send money for someone you don't know and trust !



CM  
Uwe Dotzauer  
703-340-6230



# This just in.....Mail carriers are being robbed !



CM  
Uwe Dotzauer  
703-340-6230



# Check Washing

- Deposit mail before last pickup or at the Post office directly
- Retrieve mail frequently
- Hold mail at Post Office

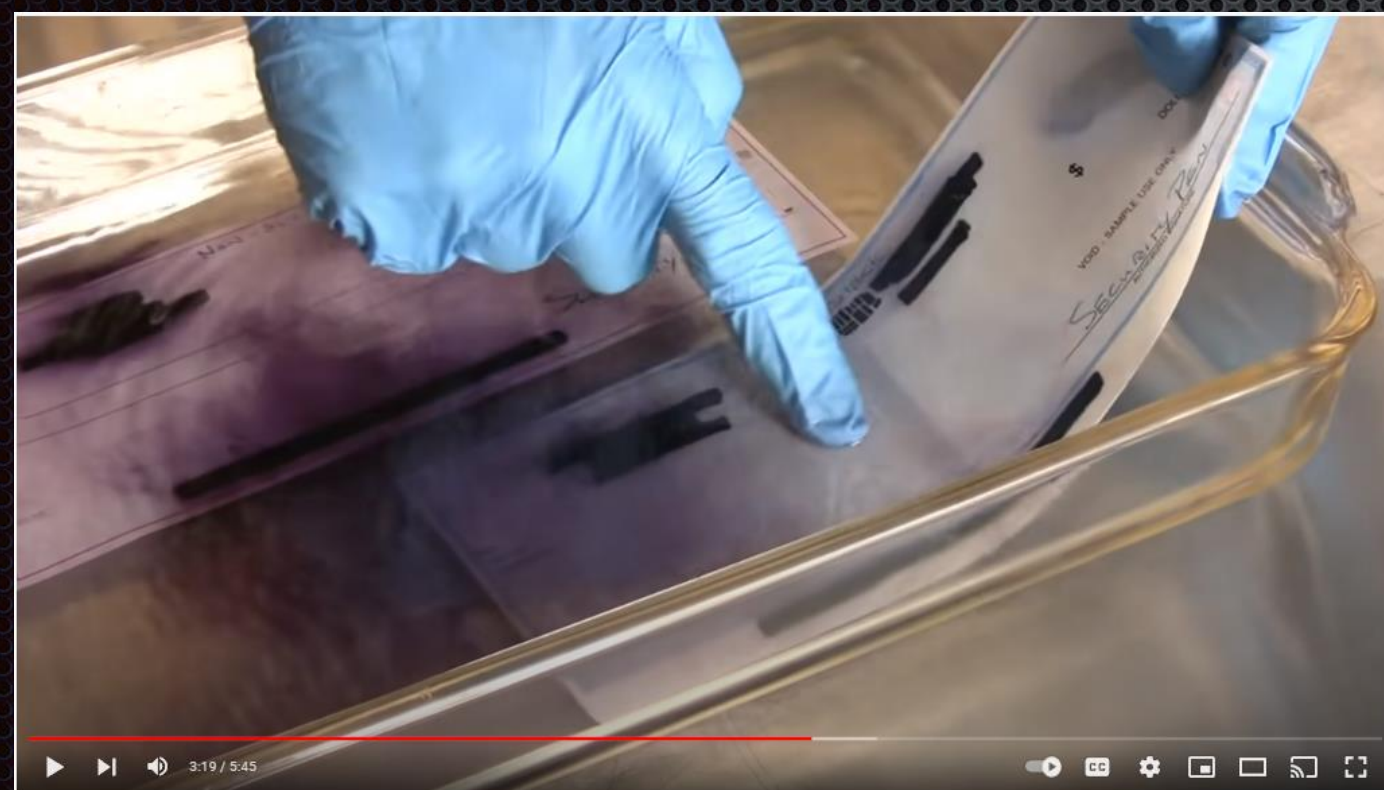

**Mailbox Fishing Leads to Check Washing!**

**Check Washing** is a process in which thieves use common household products to alter checks they recently stole out of mailboxes. They then make the checks payable to themselves or other parties.

**What can you do to prevent your checks from being altered?**

- Use a pen with pigmented ink to write checks. The ink is not easy to alter.
- Shred any voided or incorrectly written checks.
- Check your account balance frequently to ensure checks were cleared by the establishment that you wrote them out to. Note that thieves usually re-write the check for the original amount you wrote, but simply change the payee name.

**NYPD** Crime Prevention Division



- Setup Bill pay with Online Banking



CM  
Uwe Dotzauer  
703-340-6230



# Phone Scam

IRS / FBI

Grandparent

Telemarketer

Police

Tech Support

Virtual Kidnapping



CM  
Uwe Dotzauer  
703-340-6230





# Social Engineering



Use of social skills to obtain information in order to compromise a computer system

- Phishing ( Email )
- Vishing ( Phone )
- Smishing ( Text )

**Never give out any information about you, others and your organization to unknown people !**



CM  
Uwe Dotzauer  
703-340-6230



# Phishing Email

Lottery

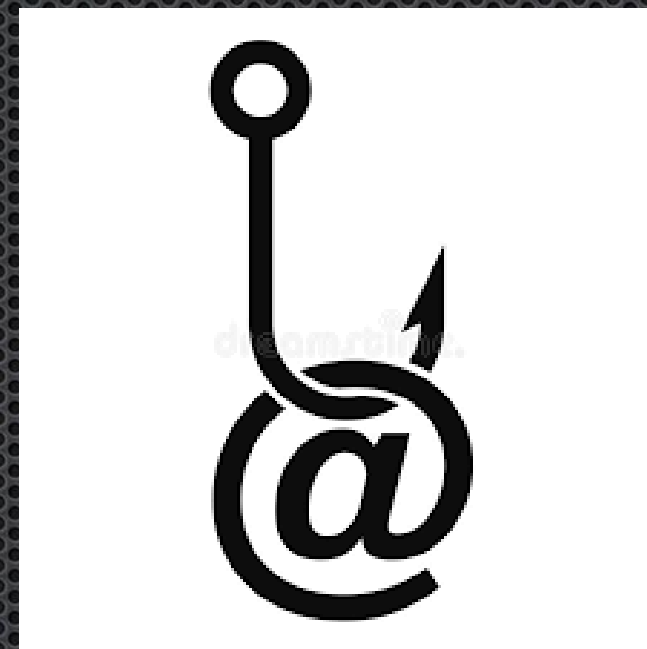
Prize

Nigerian Prince

Fake Charity

Online Dating

Investment





# Examples

This might be a phishing message and is potentially unsafe. Links and other functionality have been disabled. Click here to enable functionality (not recommended).

From: PayPal [service@paypal-australia.com.au] : 24 AM  
To: [redacted]  
Cc:  
Subject: Your account has been limited

**1. Fake sender domain.  
(not service@paypal-australia.com.au)**

**2. Suspicious Subject and content.**

**PayPal™**

**How to restore your PayPal account**

Dear PayPal member,  
To restore your PayPal account, you'll need to log in your account.

**3. Bad grammar**

It's easy:

1. Click the link below to open a secure browser window.
2. Confirm <http://69.162.70.169/ppau/> the account, and then follow the instructions.

**4. Hovering over link reveals suspicious URL.**

[Log in your account now](#)

PayPal Email ID PP32260008777636





# Examples

The image shows a screenshot of a phishing email with several annotations in blue boxes and arrows pointing to suspicious elements:

- office-365@security.onmicrosoft.com**: Fake Email, Easy to Miss
- Re: Your Office 365 account is about to be deleted**: Subject line
- To: XXXX XXXXX**: Recipient information
- invoice.pdf 2 MB**: Contains Virus
- Dear Customer**: Generic Greeting
- Please sign into the Office 365 Admin Center to pay your invoice due now!**: Demanding
- View this message in the Office 365 message center**: Suspicious Link (points to <http://57.167.145.165/invoice>)
- To customize what's included in this email, who gets it, or to unsubscribe, set your message center preferences.**: Suspicious Link
- Edit release preferences**: Poor Grammar
- Choose the release track for your organization. Use these settings to join First Release if you haven't already.**: Text
- Microsoft respects your privacy. To learn more, please read our [Privacy Statement](#).**: Text
- Microsoft Corporation  
One Microsoft Way  
Redmond, WA, USA, 98052**: Text
- [Unsubscribe](#)**: Text





# Examples

**From:** Amazon.com <adap@sci.ng>  
**Sent:** Tuesday, July 21, 2020 [Time sent is redacted.]  
**To:** [REDACTED]>  
**Subject:** [Summary Report Alert ] Statement Review Alert: Your Amazon has been locked [ Today Information ] - [New explanation added] [Summary Service Added] Automatic Email Statement Update : New sign- in [REDACTED]



**Your Amazon account is locked and order(s) are on hold.**

**We noticed some unusual activity on your account. To prevent potential misuse of your payment instrument, we have placed your order(s) on hold and locked your account.**

**Login Details:**

Date and Time: 21/07/2020 [Time sent is redacted.]  
Browser: Google Chrome  
Location: Indonesia  
IP : 155.200.234.51

Because of this activity, we processed charges in the amount of **\$732.18 USD** on your credit or debit card.

To unlock your account and receive a refund. You will also need to:

- Re-enter any addresses that you added to your account.
- Re-enter your complete credit or debit card number.

To complete the process. Click the link button below to log in to Amazon account and continue with the verification steps that will be followed by the terms and conditions.

[Verify Now](#)

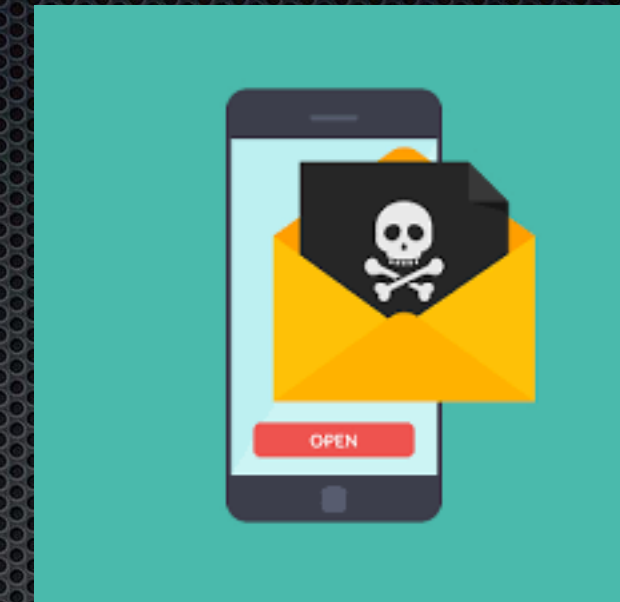
Thanks for using Amazon  
**Amazon Security Team**



CM  
Uwe Dotzauer  
703-340-6230



# SMiShing



○ Bank

○ Paypal

○ IRS

○ Service Provider





# Examples

Monday, September 28, 2020

Get Qsymia (phentermine and topiramate extended-release) CIV delivered through Qsymia Engage. See <http://r.3c.com/NQY5E5MN>. Text STOP to end HELP for info.

12:02 PM

Monday, May 11, 2020

Roni, as a part of a nationwide test we are distributing free accounts with access to Netflix + Disney+ content, go to [i673ns.info/oWUk2Yihk5](http://i673ns.info/oWUk2Yihk5)

MMS 11:36 AM

Thursday, April 23, 2020

Roni Records indicate you are overpaying on your electric bill. New tech lets you slash it in half. [qp4knt.com/mQ1M5](http://qp4knt.com/mQ1M5) EgkMQg Txt Stop to End .

11:59 AM

Thursday, April 2, 2020

Special\_Alert: New Requirements Are\_Leaving Drivers Shocked <http://ng.safe11roads.host/plau402t/BkVpLhJ> Reply2Haltk k

6:29 PM

Friday, July 17, 2020

- Your Profile suggests that you may want aid during tough times like now? Confirm, reply with 'GO' IF you need us to send U aid and grant programs.

10:35 AM

Saturday, April 25, 2020

Roni, melt your excess weight away with this Shark Tank miracle product. Completely free for the first 10 [q72b1.info/uxuRM59EqE](http://q72b1.info/uxuRM59EqE)

MMS 4:14 PM

Thursday, April 9, 2020

Is this Roni Bliss? We have a free iPhone for you. Can you confirm your details by today: [j6vq04p.info/XmuLv0oPHO](http://j6vq04p.info/XmuLv0oPHO)

MMS 7:06 PM

Friday, April 3, 2020

Package theft is up 400%, How to Stop <http://pe.net3reporting.host/rightwelcm/BkVpLhJ> Reply-To-sto,p.

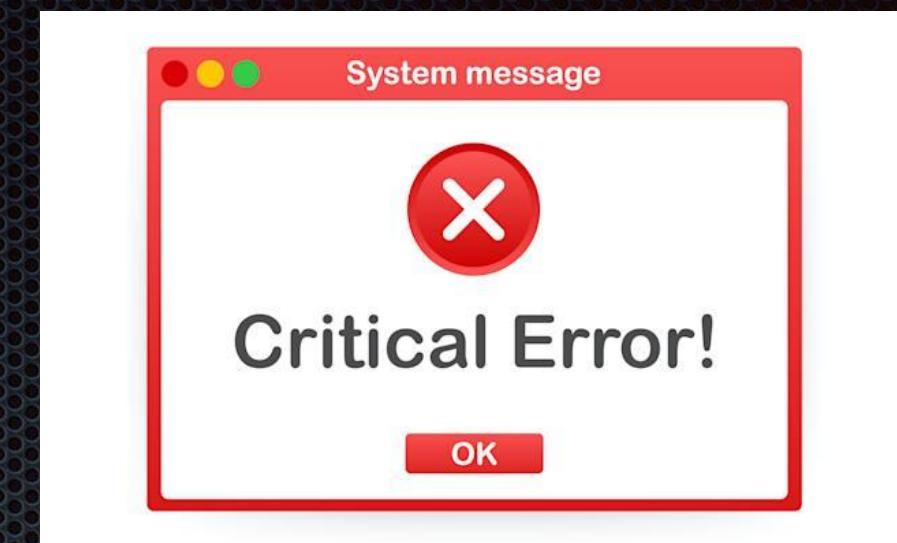
1:50 PM







# Pop-up Adware



Did you click and install a “ free “ application ?

- Advertisements appear more and more
- Homepage changes
- Web-links are redirected
- Web browser is slow
- Browser crashes



CM  
Uwe Dotzauer  
703-340-6230



# Example



WARNING: EMAIL SCAN! x

← → ↻ 🏠 📄 [Redacted URL] ☆ ☰

 **WARNING!**

**YOUR E-MAIL INBOX IS INFECTED:**

System Detected (2) Potentially Malicious E-Mail Viruses: *Email-Worm.Web.FakeLogin* and *Email.Spy-Password*. Your Password, Personal & Financial Information **IS NOT SAFE.**

**To Secure Your E-Mail Passwords, Call Tech Support Now:**

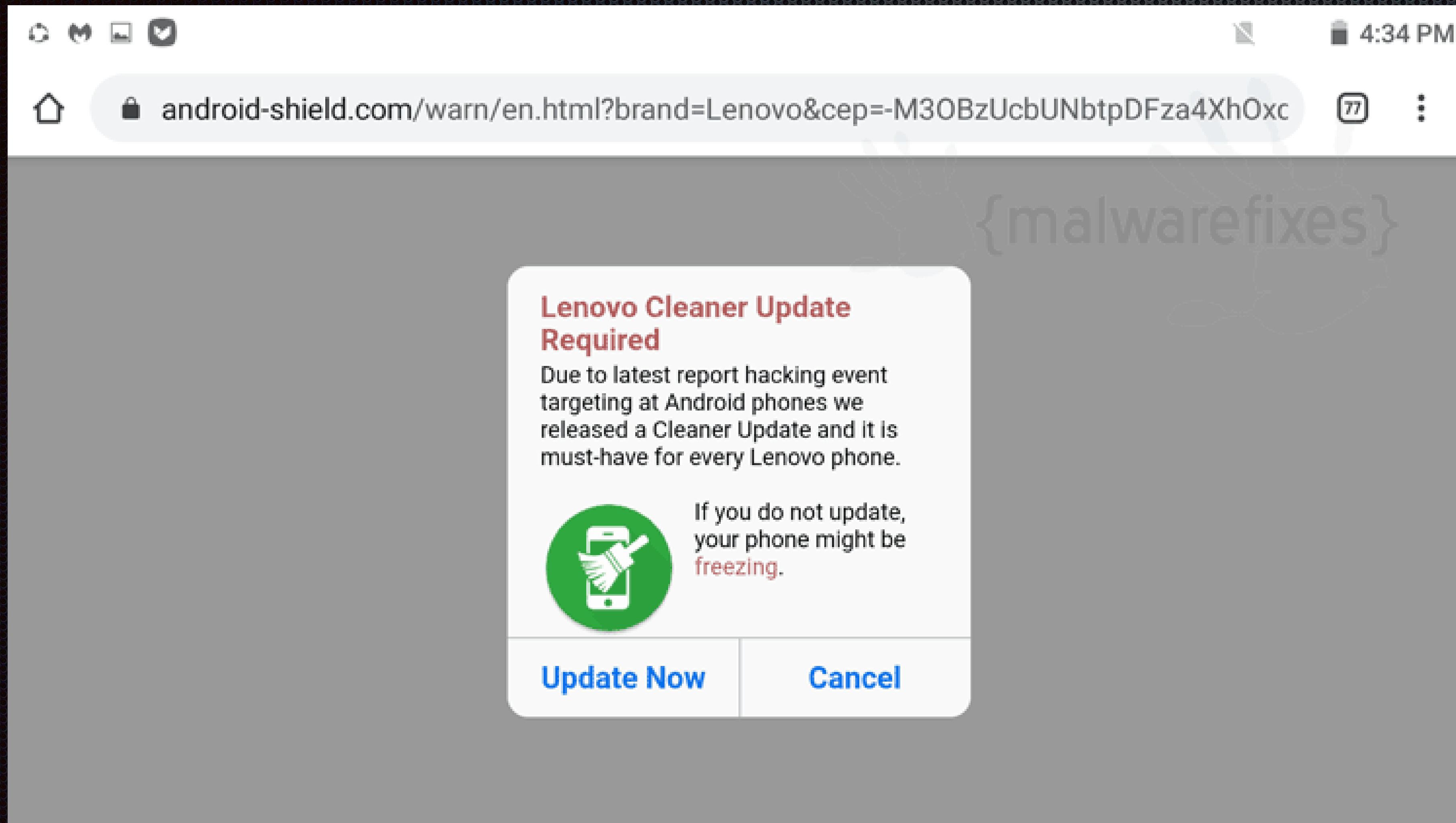
**1(855) 815-4689**  
(High Priority E-Mail Recovery Line)

Your IP Address: [Redacted] | Generated on 05-22-2014 | Priority: Urgent






# Example



The screenshot shows a mobile browser interface. At the top, there are navigation icons (back, forward, home, search) and the time 4:34 PM. The address bar contains the URL: `android-shield.com/warn/en.html?brand=Lenovo&cep=-M30BzUcbUNbtpDFza4XhOxc`. The main content area is a grey background with a white dialog box in the center. The dialog box has a title "Lenovo Cleaner Update Required" in red. Below the title is a paragraph of text: "Due to latest report hacking event targeting at Android phones we released a Cleaner Update and it is must-have for every Lenovo phone." To the left of the text is a green circular icon with a white smartphone and a hand holding a brush. To the right of the icon is the text: "If you do not update, your phone might be freezing." At the bottom of the dialog box are two buttons: "Update Now" and "Cancel".

**Lenovo Cleaner Update Required**

Due to latest report hacking event targeting at Android phones we released a Cleaner Update and it is must-have for every Lenovo phone.

 If you do not update, your phone might be freezing.

[Update Now](#) [Cancel](#)





# Example

## (1) Mac OS Browser warning:

### Your computer might be infected with adware!

Your location:  
Las Cruces, NM

Date:

Monday, January 02, 2015



<http://www.mac-tech-alerts.com>

Suspicious Activity Found On Your Computer, Due to  
Pop-Up Advertisement Windows and Invasive Links.

Please Contact Certified Live Technicians  
1-855-809-6230 (Toll Free)

OK

### What to do

Call **855-809-6230**

with removing

viruses. (Toll-FREE, High Priority Call  
Line)

### More Information:

Seeing these pop-up's means that you may  
have adware installed on your computer  
which puts the performance of your  
computer at a serious risk. It's strongly  
advised that you call the number above to  
get your computer fixed before you continue  
accessing the internet.

**24/7**

UNMATCHED SERVICE AND SUPPORT.



Your computer might  
be infected with adware:

Pop-up windows that  
pop up randomly.

2. Strange links or menus appear  
in the browser.
3. Unauthorized release of files,  
usually via e-mail.
4. A sudden decline in PC or  
Internet performance.
5. Programs not opening or  
taking a long time to start.



CM

Uwe Dotzauer

703-340-6230



# Tech Support Scam

- \* COLD phone calls
- \* Adware pop-up
- \* Online ads





# Ransomware



- Attachments
- Links in email
- Free applications



Demand of money in exchange for YOUR data





# Example

## YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)

Following violations were detected:

Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.

This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of \$200.

You have 72 hours to pay the fine, otherwise you will be arrested.

You must pay the fine through [REDACTED]

To pay the fine, you should enter the digits resulting code, which is located on the back of your [REDACTED] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

If an error occurs, send the codes to address [fine@fbi.gov](mailto:fine@fbi.gov).



OK





# Example

helpdecrypt@msgsafe.io



## YOUR FILES ARE ENCRYPTED

Don't worry, you can return all your files!  
If you want to restore them, follow this link: email [helpdecrypt@msgsafe.io](mailto:helpdecrypt@msgsafe.io) YOUR ID **C279F237**  
If you have not been answered via the link within 12 hours, write to us by e-mail: [helpdecrypt@msgsafe.io](mailto:helpdecrypt@msgsafe.io)

**Attention!**

- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.





# Romance Scams

Did you ever meet the person you are meeting online ?

Money Talk ?

Get “ Proof of Life “







# Online Shopping



- Design of Website
- Suspicious / Strange Domain Name
  - Product descriptions
  - Impossibly Low prices
  - Payment method
- No or unclear contact information





# Example

NEW ARRIVAL

SATCHELS

SHOULDER BAGS

TOTES

VALUE SPREE

WALLETS

**New Products**

**Product Details**

**Coach In Signature Large Gold Wallets ARZ**  
This capacious new wallet silhouette showcases the smooth hand of luxurious glove-tanned leather in a refined design.

**Coach Madison Madeline East West Large Grey Satchels BXE**  
\$65.00 \$248.00

**Coach Madison Madeline East West Large Grey Satchels BXE**





# Example

www.bottomheels.com/pc

www.bottomheels.com/pcmyorder/myorder.php

Language: English

VERIFIED by VISA MasterCard SecureCode

OrderID: Withred8032-146-1449674603 Amount: USD 189 Thanks for your shopping on www.bottomheels.com

Credit Card Information

Card Type:  VISA  MasterCard  JCB

Credit Card No:

Expiry Date: 1 / 2015

CVC/CVV2:

Billing Address

No Encryption (Https)  
on Payment page





Hold on a minute.....



CM  
Uwe Dotzauer  
703-340-6230



# ....but I thought I am secure !



**SEEMS SECURE**  
AGAINST ANYONE INCAPABLE OF USING SCISSORS

DIY.DESPAIR.COM



Username : admin  
Password : admin



**SECURITY FAIL**



**SECURITY FAIL**



CM  
Uwe Dotzauer  
703-340-6230



# How can WE prevent being a victim ?



CM  
Uwe Dotzauer  
703-340-6230



# Computer

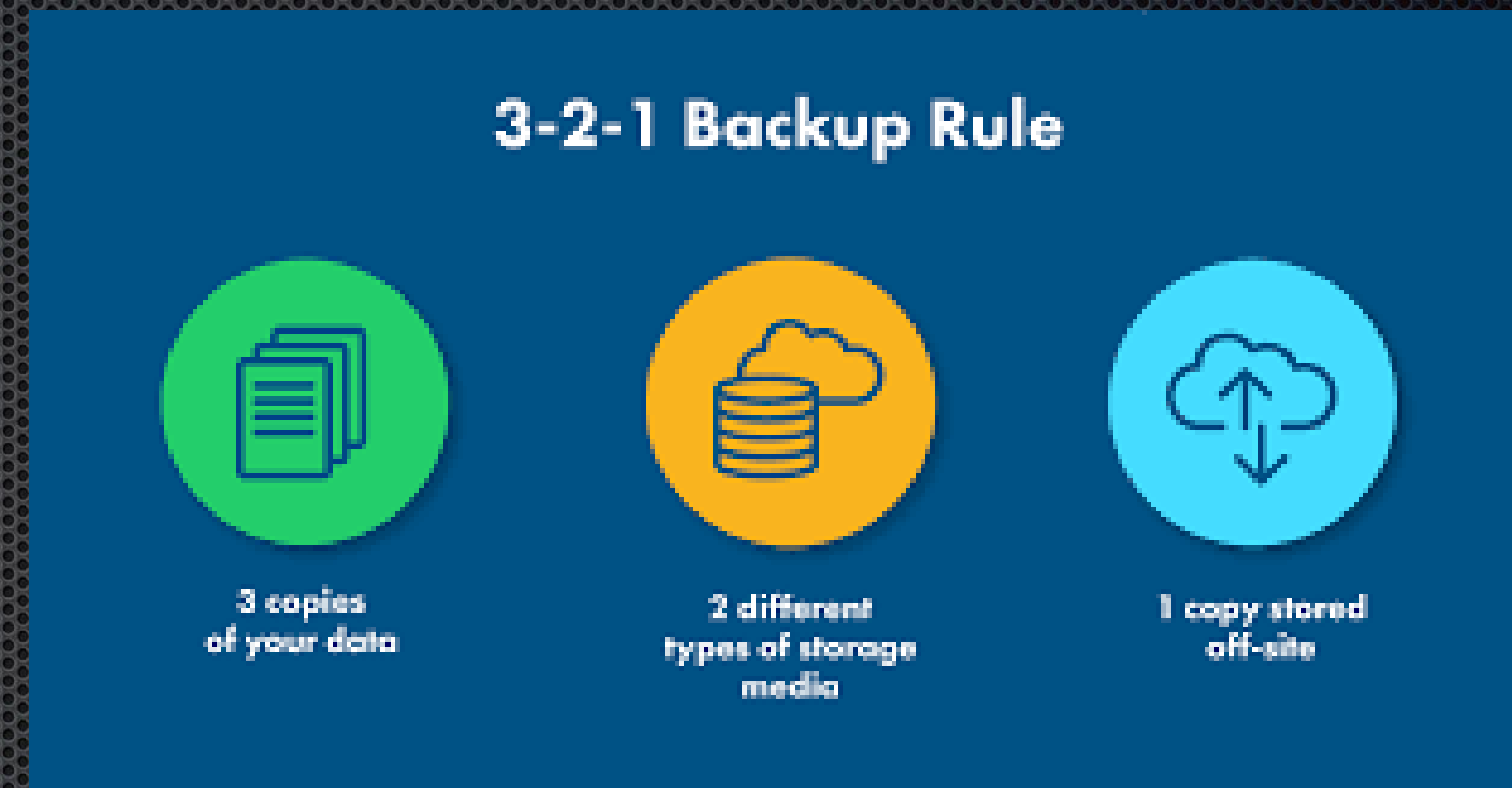
- Keep up with OS updates / upgrades
- Safari, Chrome other Browser Software
- Firewall
- Password Manager / Safari
- Internet Security Suite
- Malware Scanner
- True Online Backup





# Backup is your life line !

iCloud and OneDrive is NOT backup !





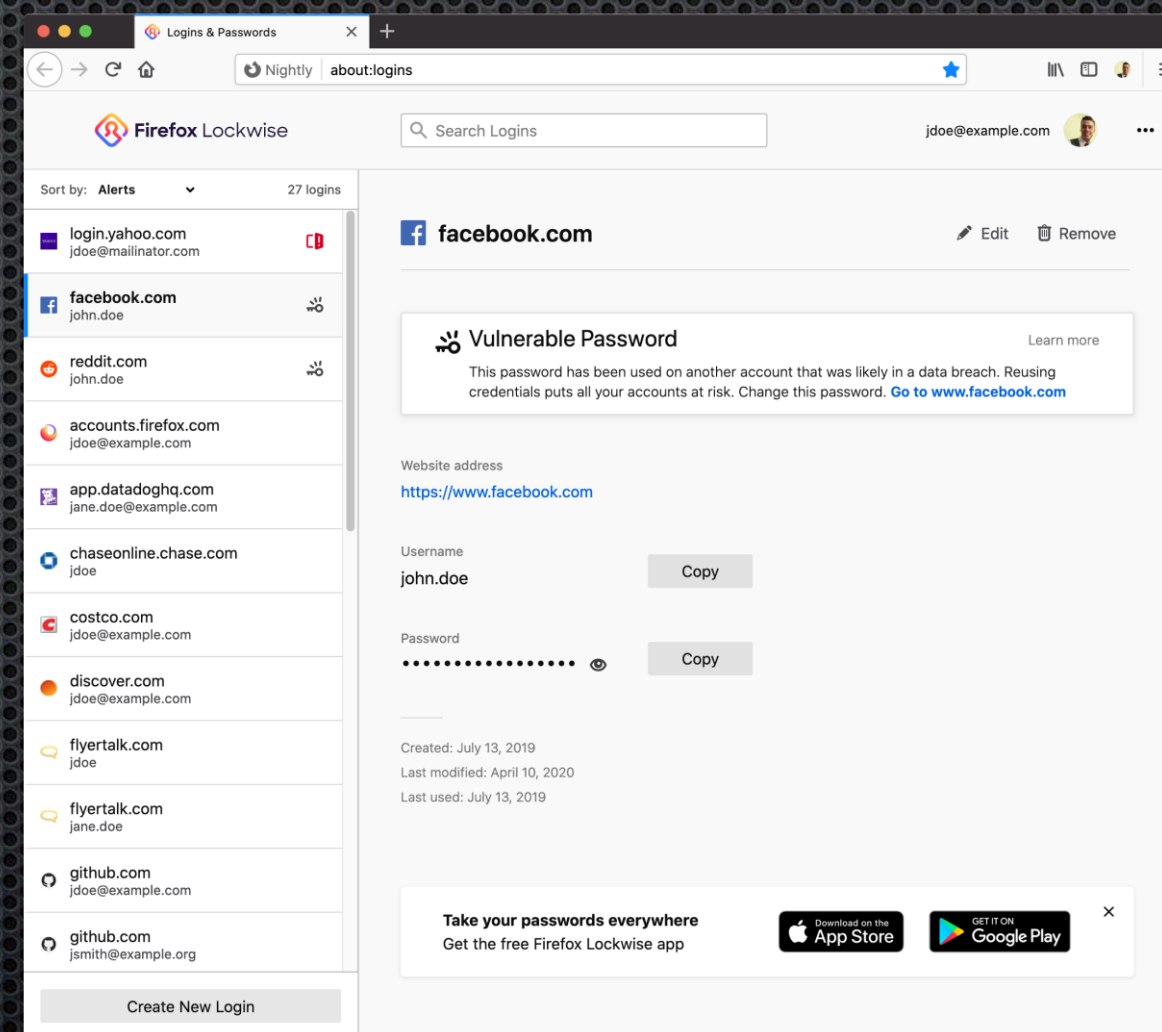
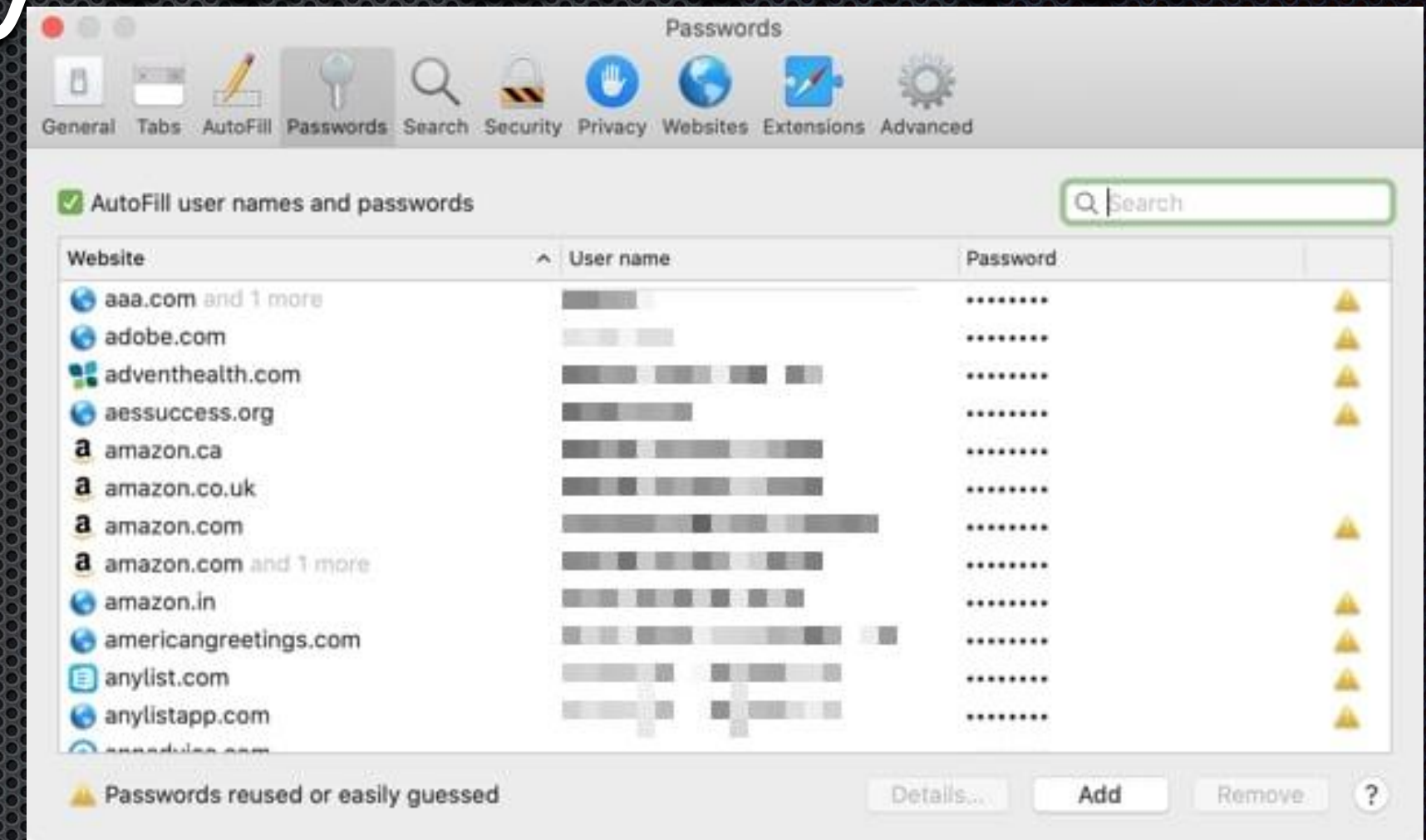
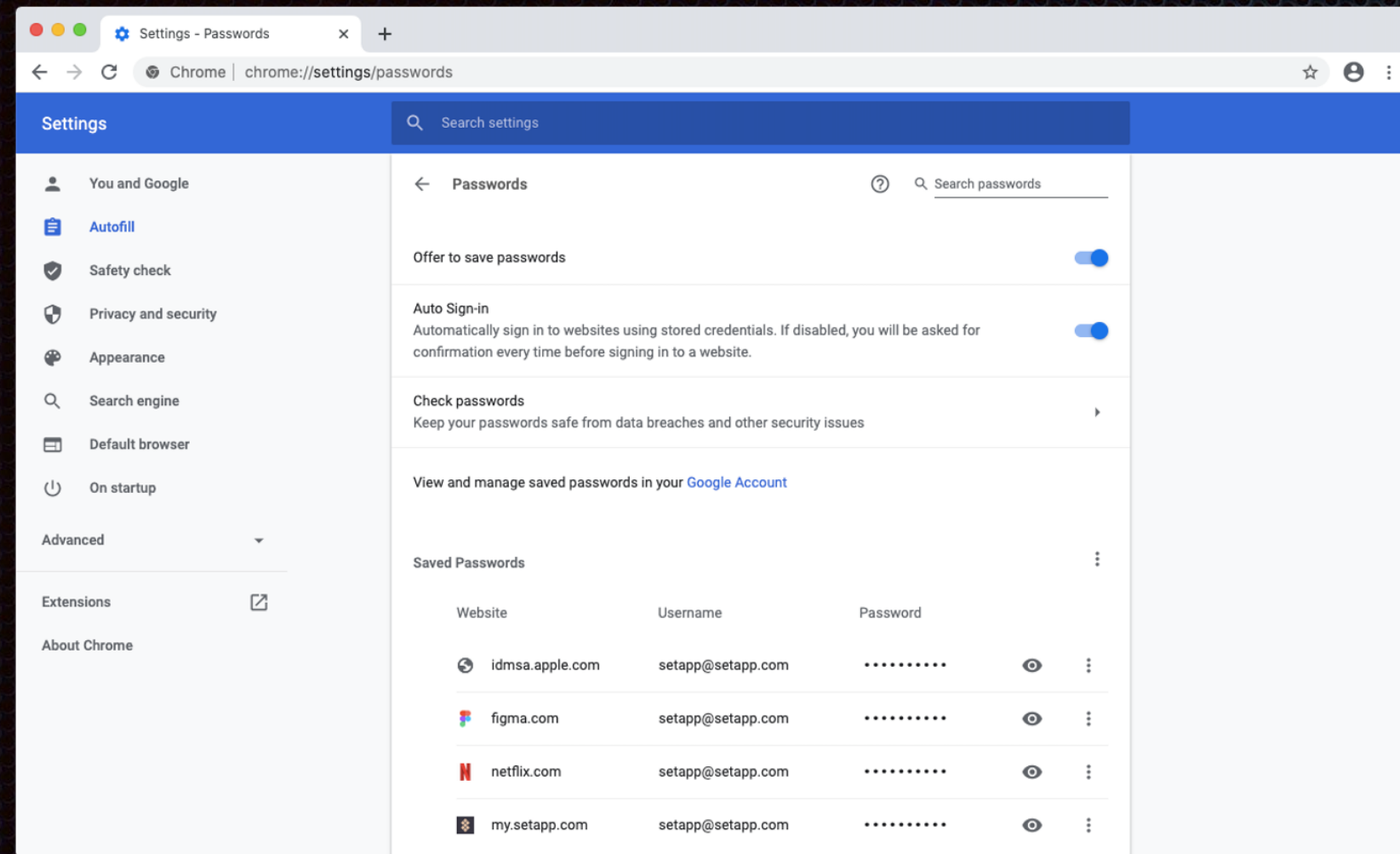
# The Password “Complex”

- Longer is better ( 16 characters )
- Add some special ones ( \* & ^ \$ )
- Be unique ! ( Don't reuse )
- Password Generator
- Change them regularly





# Password Managers in your Browser





## Treat your passwords like your underwear

- Never share them with anyone
- Change them regularly
- Keep them off your desk

Be aware of the new European law on privacy and personal data, General Data Protection Regulation – effective 25 May 2018

[www.maastrichtuniversity.nl/privacy](http://www.maastrichtuniversity.nl/privacy)

Do it like the Dutch !!!!





# Check if your Password has been exposed



[Firefox Monitor](#)

[Pwned](#)

[Avast Hack Check](#)



Check your Google or Safari Browser



CM  
Uwe Dotzauer  
703-340-6230



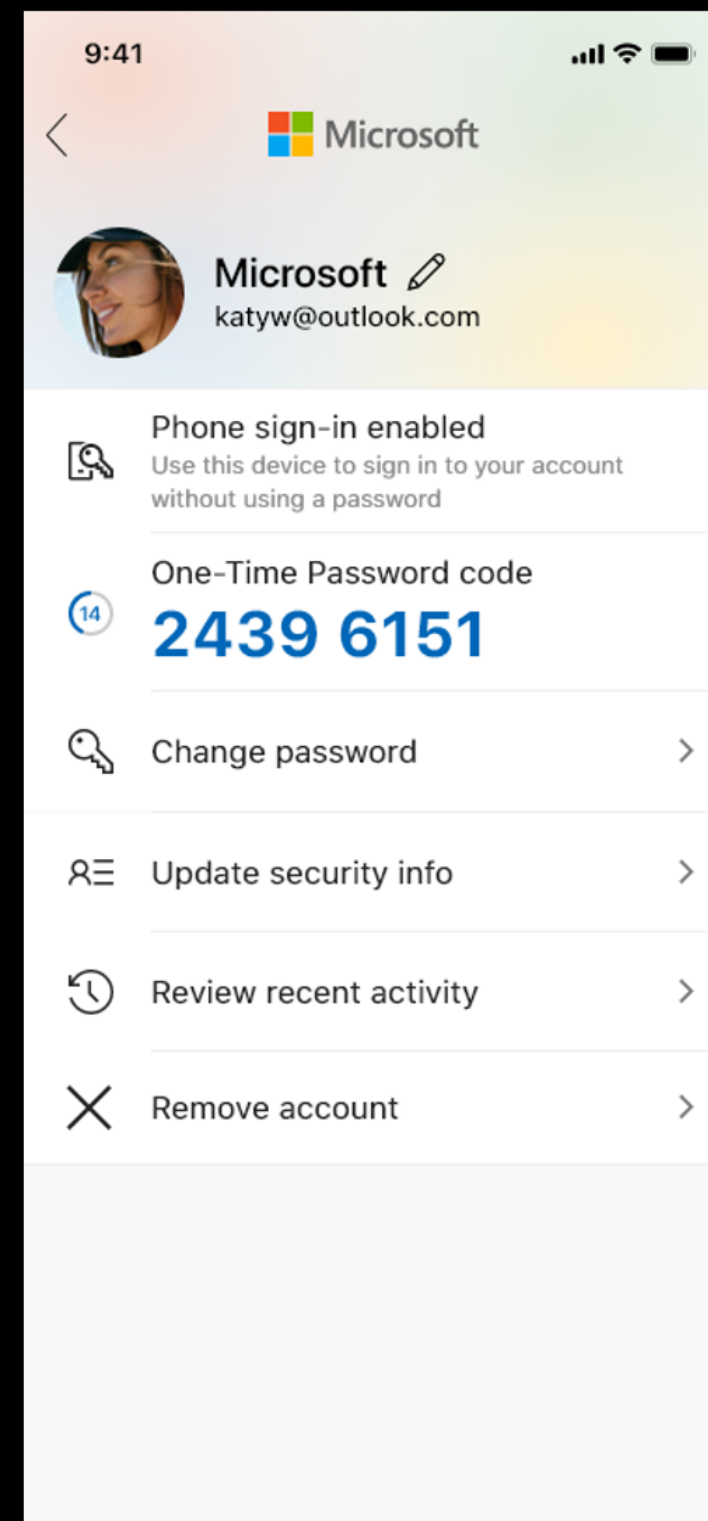
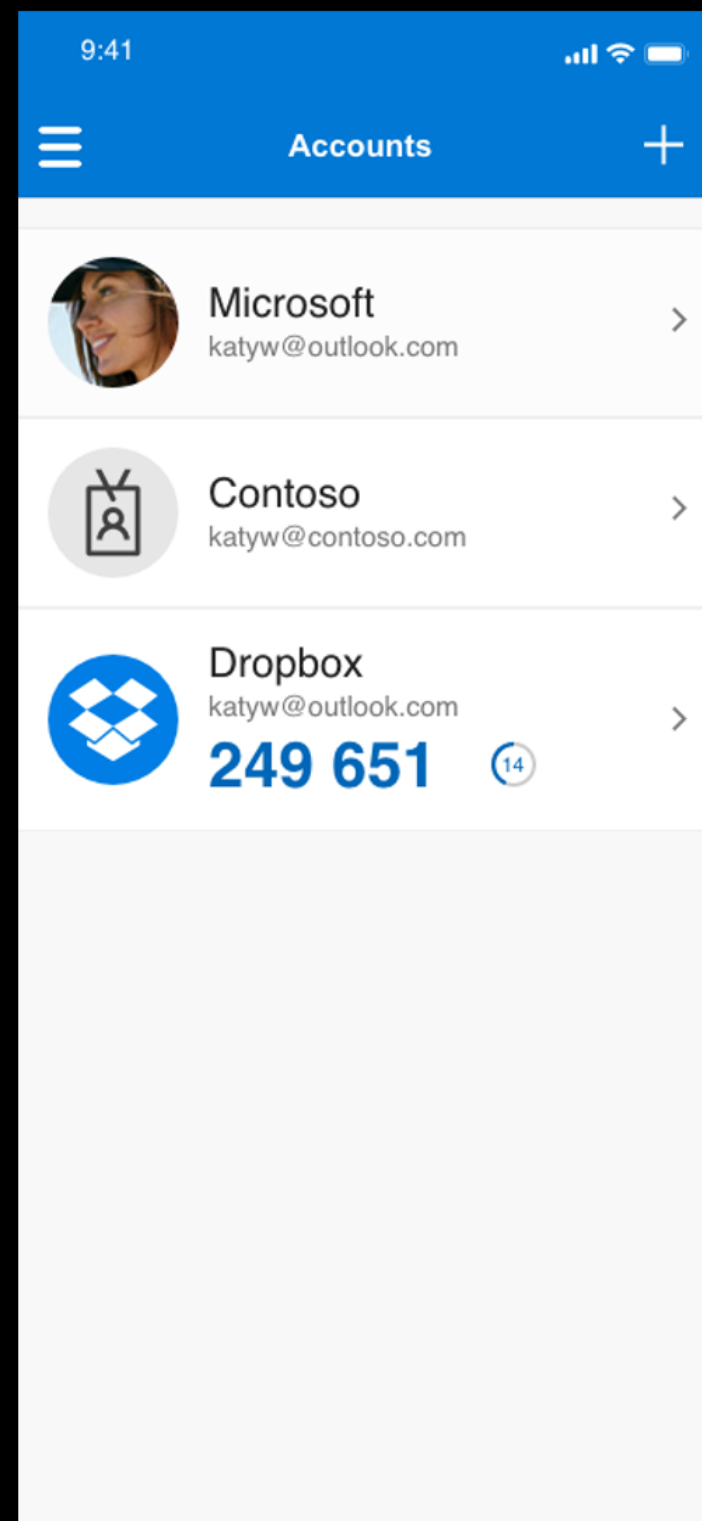
# Online Account Safety

- ✓ Two factor Authentication
  - ✓ SMS/Text
- ✓ Authenticator much better
- ✓ Password Manager





# Example





# What else ?



CM  
Uwe Dotzauer  
703-340-6230



# Knowing is ....preventing

Sign up for free newsletters



[Scamicide](#)

[SANS Institute](#)



[InfoSecurity Magazine](#)

[AARP Watchdog alert](#)

[FRAUD.org](#)

[Local Law Enforcement](#)



CM  
Uwe Dotzauer  
703-340-6230



# Freeze your credit



Freeze your credit over the phone by contacting each of the three credit bureaus.



EXPERIAN

888-397-3742



EQUIFAX

800-349-9960



TRANSUNION

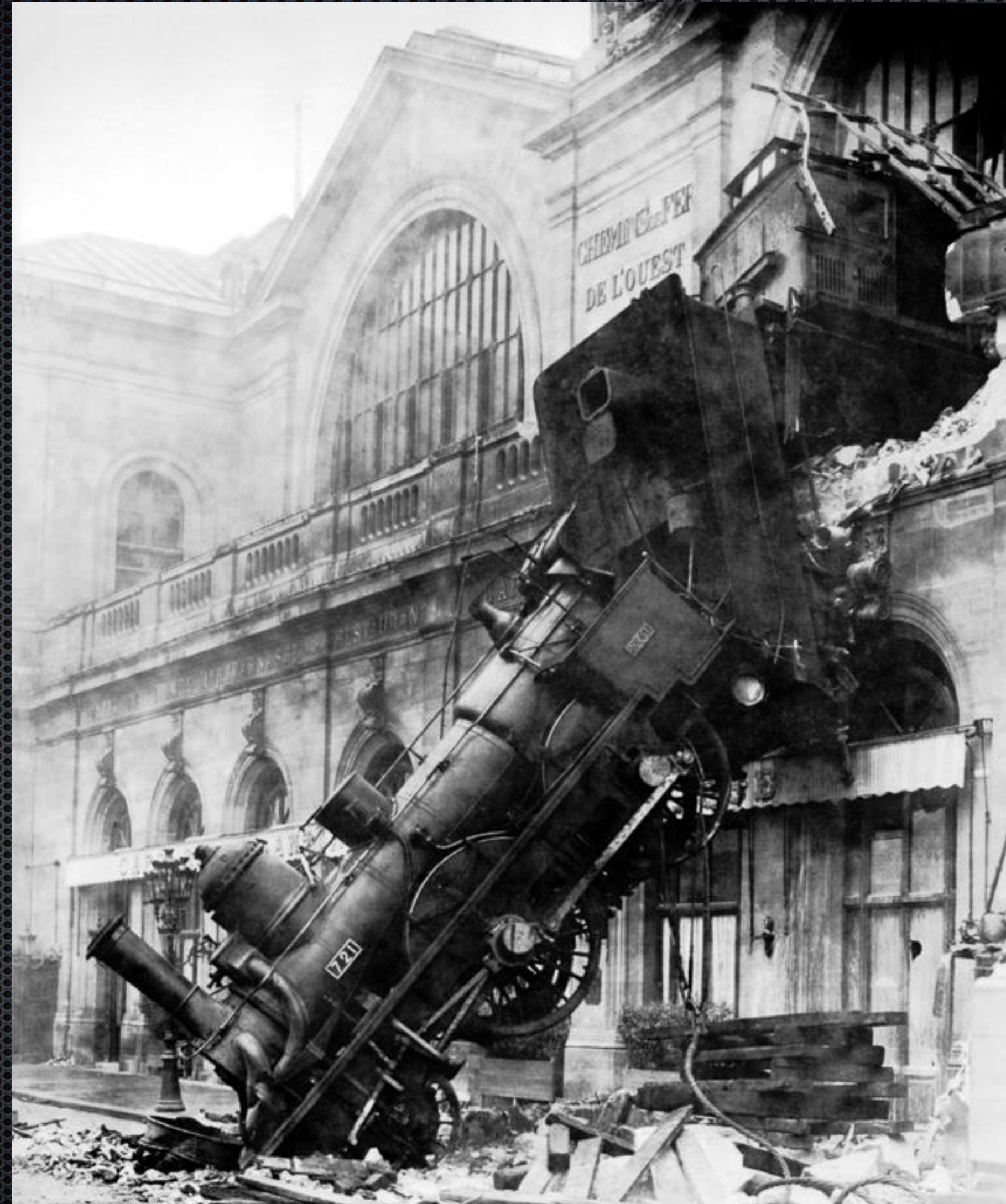
888-909-8872



CM  
Uwe Dotzauer  
703-340-6230



# OK...It happened..What now ?



CM  
Uwe Dotzauer  
703-340-6230



# Call a professional

<https://www.identitytheft.gov/#/Steps>

Bank

Credit Card Company



CM  
Uwe Dotzauer  
703-340-6230



# Report the online scam !!!!

## FBI

# Internet Crime Complaint Center IC3

<https://www.ic3.gov>



**FEDERAL BUREAU OF INVESTIGATION  
Internet Crime Complaint Center IC3**



CM  
Uwe Dotzauer  
703-340-6230



# The Take Away

1. Be always skeptical and suspicious
2. Keep OS and iOS updated
3. Don't give out any information over the phone nor email (Stranger Danger)
4. Ask a professional
5. Never give out your Password !!!







CM  
Uwe Dotzauer  
703-340-6230



# Questions ?

( I am sure you have at least one )

CONTACT:

[uwe007@hotmail.com](mailto:uwe007@hotmail.com)

703-340-6230

( consulting services can be provided )



CM  
Uwe Dotzauer  
703-340-6230