View this email in your browser

Kerno.biz LLC Newsletter **February 2022**

In honor of Identity Theft Awareness Week 2022, I thought this would be a good time to write a current newsletter on the subject. I have written about this in the past, but in the last few years, there has been a sharp rise in the number of fake emails, text messages and computer pop-up messages. A number of my clients, as well as organizations around the world, have been tricked into clicking on links and calling phone numbers that they should not. The bad guys are getting more and more sophisticated and can easily trick anyone if we are not careful. This month it would be helpful to go over what to look out for and how to preemptively protect yourself and your devices.

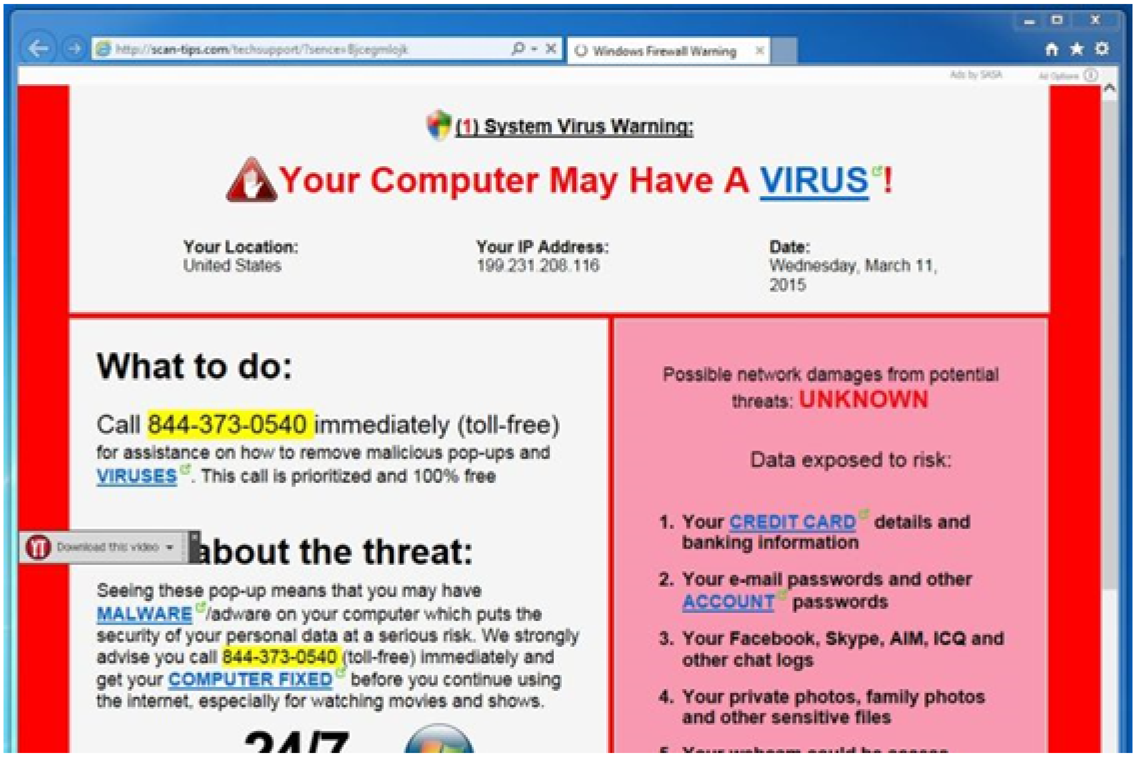
In this month’s newsletter I will provide information on:

- How to protect yourself from identity theft
- How to freeze your files to protect your identity:
    - Credit files
    - Utility file
    - Federal tax return
- How to obtain free credit reports (to monitor for identity theft)
- Security checklist for you and your technology click here for PDF version or DOC version

What is phishing and malware

Please watch this 2 minute video: Microsoft - Protect yourself from tech support scams

“Phishing text messages and emails have become a dangerous yet unavoidable threat in the digital age. Your best protection is to err on the side of caution and use the “delete” button on emails and texts that seem sketchy. Remember, a legitimate organization or business will never ask you to share sensitive, personal information via insecure channels like email, text or pop-up messages. If the message is truly important, the sender will attempt to contact you through verified methods like telephone or snail mail.” Source: Aging Care - 5 Steps to Take After Clicking on a Phishing Link



(1) System Virus Warning:

Your Computer May Have A VIRUS!

Your Location:
United States

Your IP Address:
199.231.208.116

Date:
Wednesday, March 11, 2015

What to do:

Call 844-373-0540 immediately (toll-free)
for assistance on how to remove malicious pop-ups and VIRUSES. This call is prioritized and 100% free

about the threat:

Seeing these pop-up means that you may have MALWARE/adware on your computer which puts the security of your personal data at a serious risk. We strongly advise you call 844-373-0540 (toll-free) immediately and get your COMPUTER FIXED before you continue using the internet, especially for watching movies and shows.

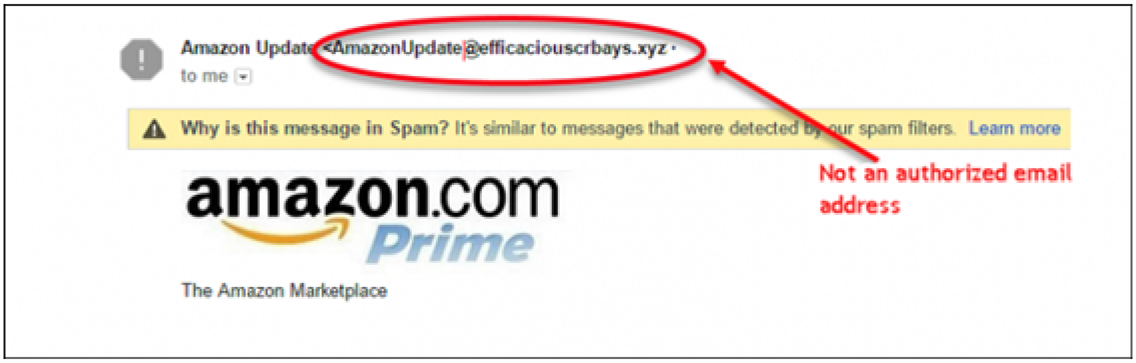
24/7

Possible network damages from potential threats: UNKNOWN

Data exposed to risk:

1. Your CREDIT CARD details and banking information
2. Your e-mail passwords and other ACCOUNT passwords
3. Your Facebook, Skype, AIM, ICQ and other chat logs
4. Your private photos, family photos and other sensitive files
5. Your webcam could be access

A phishing email pretending to be from (insert company name here) typically contains a link that takes you to a fake website, or a phone number to the scammers phone bank, with the goal of getting you to pay for a worthless product or service, installing malware, stealing your personal information, or worse, encrypting your files with ransomware. These emails often address is from "AmazonUpdate @ efficaciouscrbays.xyz", obviously "efficaciouscrbays.xyz" is not "amazon.com", so this email is not from Amazon no matter what it looks like.



Amazon Update <AmazonUpdate@efficaciouscrbays.xyz>
to me

⚠ **Why is this message in Spam?** It's similar to messages that were detected by our spam filters. Learn more

Not an authorized email address

In the worst case scenario, ransomware will be installed on your computer and you will not be able to access any of your files unless a "ransom" is paid. Of course, even if someone pays the ransom there is no guarantee that they will get their files back. So backups are critical if you are going to protect yourself from this type of criminal activity, and even from disasters.

The Marshall Fire in Boulder County in December 2021 is now the most destructive wildfire in Colorado history, with 991 homes destroyed. If those people did not have an off-site backup of their data, then their computers and backup drives were destroyed in the fire and they are starting over from scratch. I do not want that to happen to any one of my clients.

1. Marshall fire, Boulder County 2021 • 991 homes lost

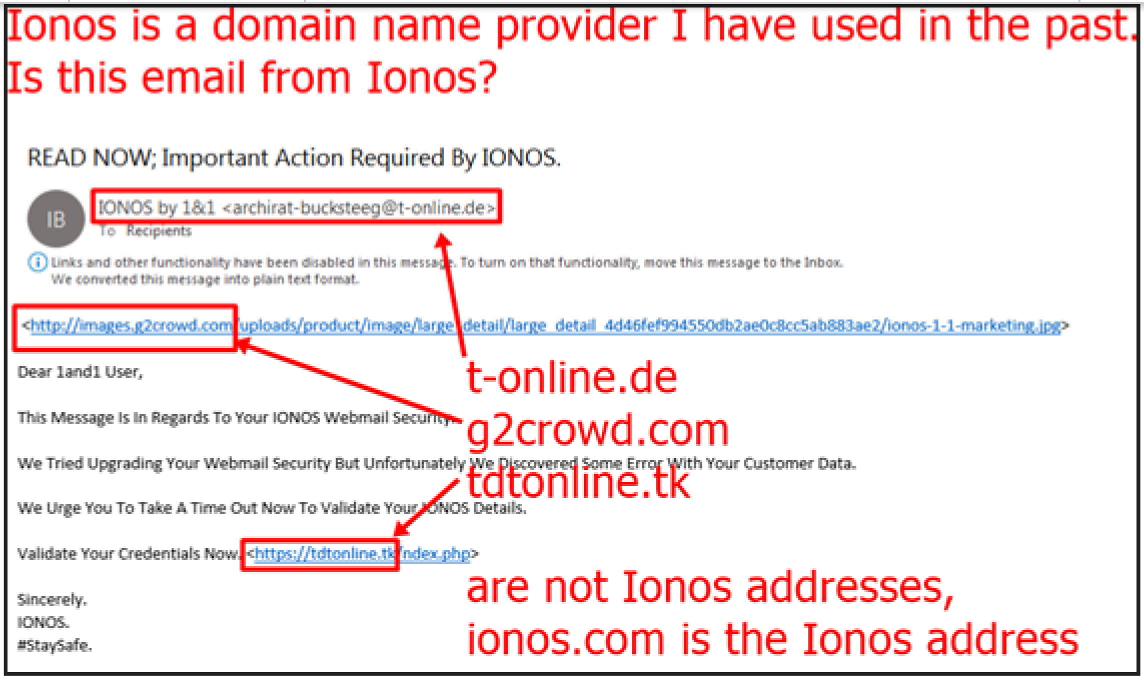
Remember, disasters can take many forms: fires, hurricanes, tornado, floods, mud slides, earthquakes, collapsed condos, gas line explosions in neighborhoods, so everyone would be wise to be prepared.

How to recognize phishing attempts

Please watch this 2 minute video: Microsoft - Protect yourself from tech support scams

Here are some typical traits of phishing scams:

- Scare you into believing there is some problem with your computer, cell phone or account.
- Ask for your personal or financial information.
- Ask you to click links or download software.
- Impersonate a reputable organization, like your bank, a social media site you use, or your workplace.
- Impersonate someone you know, like a family member, friend, or coworker.
- Look exactly like a message from an organization (has the company logo in it) or person you trust.
- They may say they've noticed some suspicious activity or log-in attempts
- They may claim there's a problem with your account or your payment information
- They may say you must confirm some personal information
- They may include a fake invoice
- They may want you to click on a link to make a payment
- They may say you're eligible to register for a government refund
- They may offer a coupon for free stuff



Ionos is a domain name provider I have used in the past. Is this email from Ionos?

READ NOW; Important Action Required By IONOS.

IB IONOS by 1&1 <archirat-bucksteeg@t-online.de>
To Recipients

ⓘ Links and other functionality have been disabled in this message. To turn on that functionality, move this message to the Inbox.
We converted this message into plain text format.

<http://images.g2crowd.com/uploads/product/image/large_detail/large_detail_4d46fef994550db2ae0c8cc5ab883ae2/ionos-1-1-marketing.jpg>

Dear 1and1 User,

This Message Is In Regards To Your IONOS Webmail Security.

We Tried Upgrading Your Webmail Security But Unfortunately We Discovered Some Error With Your Customer Data.

We Urge You To Take A Time Out Now To Validate Your IONOS Details.

Validate Your Credentials Now. <https://tdtonline.tk/index.php>

Sincerely.
IONOS.
#StaySafe.

t-online.de
g2crowd.com
tdtonline.tk
are not Ionos addresses,
ionos.com is the Ionos address

They are all 100% fake messages!

It goes without saying, but here goes, never click links, open attachments or call phone numbers in emails, text messages or pop-up messages like this. **They are all scams** trying to trick you. Ignore and delete. Instead, if you want to check if something is for real, go to the website yourself and login to check your account. If you have any question, open your browser (Chrome, Safari, Edge) and go to the real website yourself (type the website address yourself or use your previously saved bookmark/favorite). If it looks like it came from someone you know, call the person to find out if they really sent the email. But really, we already know they did not send it so save yourself the trouble. **It is much safer to do nothing then to do something. If you do nothing and something stops working down the road, we can fix that a lot easier than recovering from a scam.**

Preventive care (steps to take before disaster strikes)

- On-site: Backup of your entire computer hard drive to an external hard drive on-site
    - macOS

- Off-site: Sync and/or backup your data to a cloud service

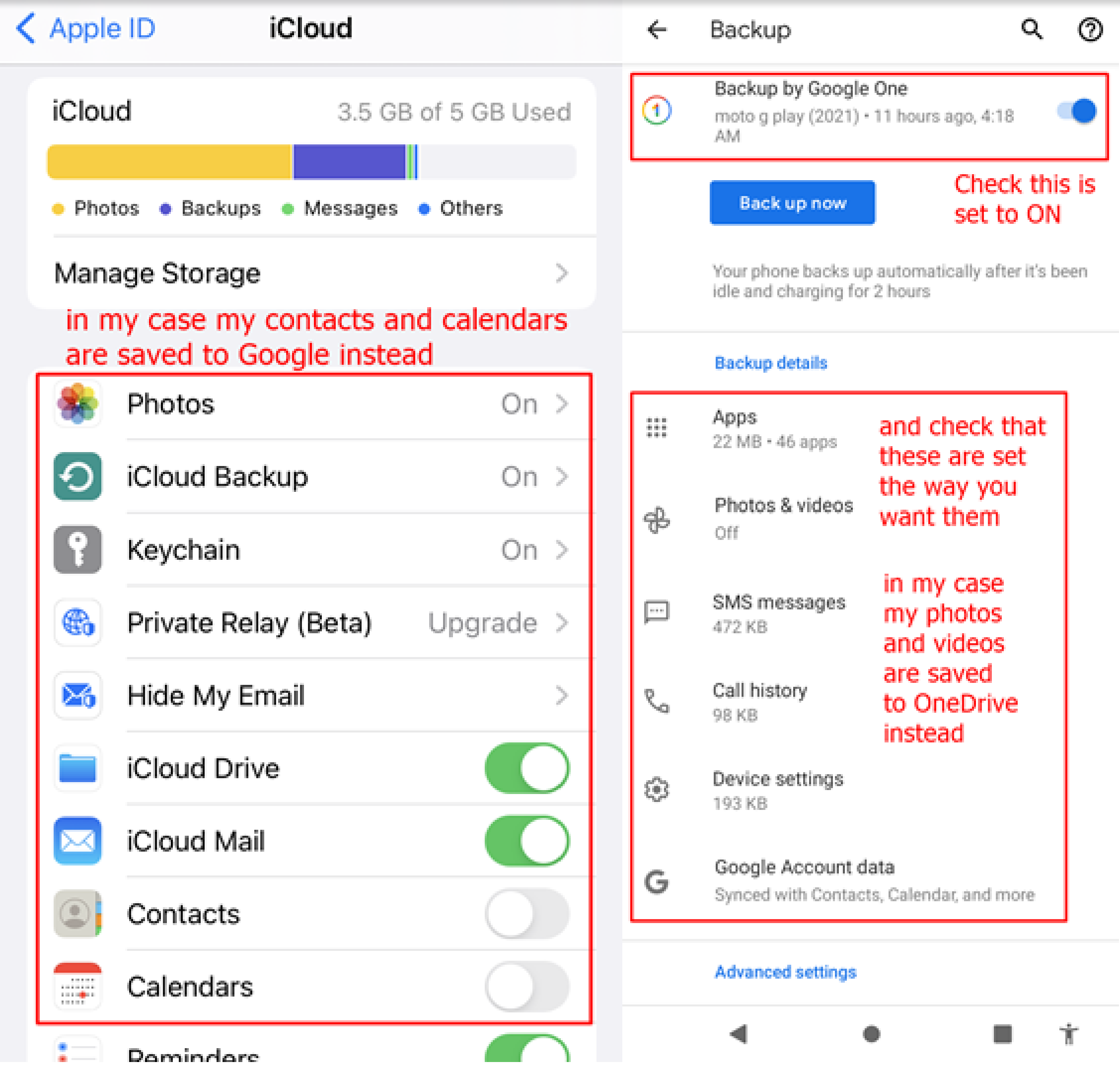
Data:

- Documents
- Photos
- Music
- Videos
- Email
- Contacts
- Calendar
- Bookmarks/favorites
- Notes
- Other app data (Quicken, QuickBooks, etc.)

Cloud services (may need to use a combination of services to cover everything):

- Apple iCloud: https://icloud.com
- Microsoft OneDrive: https://onedrive.com
- Google Drive: https://drive.google.com
- Dropbox: https://dropbox.com
- Carbonite: https://carbonite.com

- Turn on cell phone backup
  - Apple iOS (iPhone, iPad) backup
  - Google Android backup



< Apple ID   iCloud

iCloud   3.5 GB of 5 GB Used

● Photos ● Backups ● Messages ● Others

Manage Storage >

in my case my contacts and calendars are saved to Google instead

Photos	On >
iCloud Backup	On >
Keychain	On >
Private Relay (Beta)	Upgrade >
Hide My Email	>
iCloud Drive	On
iCloud Mail	On
Contacts	Off
Calendars	Off
Reminders	On

← Backup

Backup by Google One — On
moto g play (2021) • 11 hours ago, 4:18 AM

Back up now

Check this is set to ON

Your phone backs up automatically after it's been idle and charging for 2 hours

Backup details

Apps	22 MB • 46 apps
Photos & videos	Off
SMS messages	472 KB
Call history	98 KB
Device settings	193 KB
Google Account data	Synced with Contacts, Calendar, and more

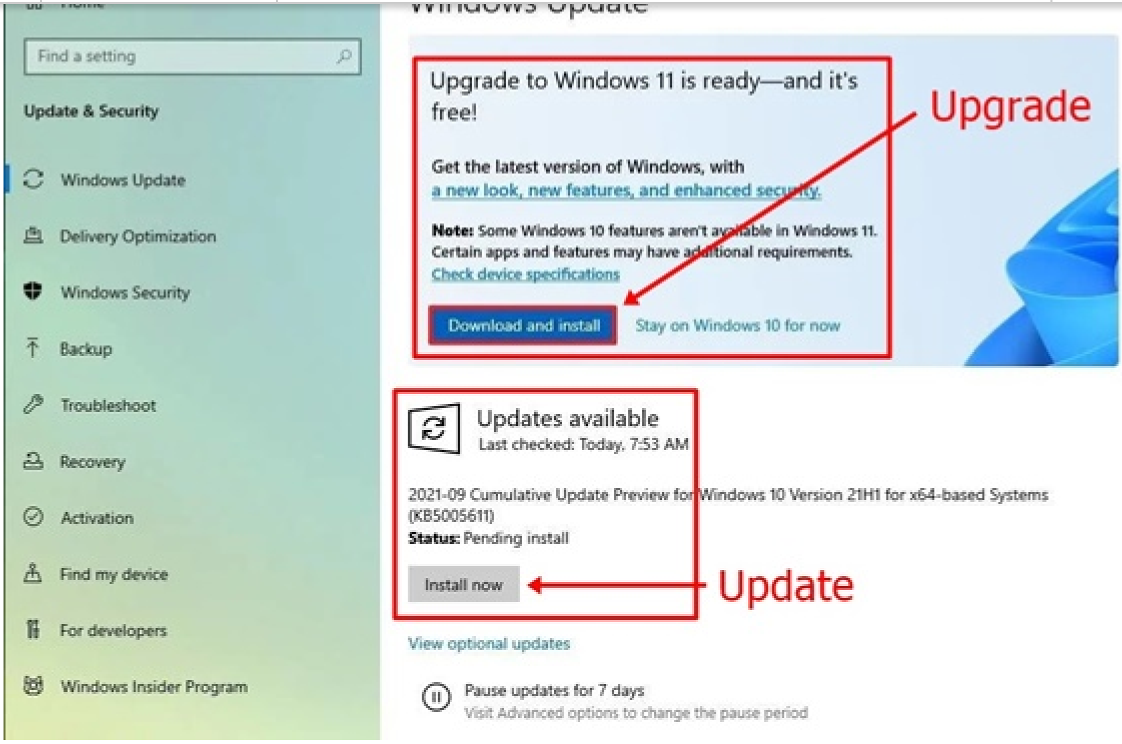
and check that these are set the way you want them

in my case my photos and videos are saved to OneDrive instead

Advanced settings

How to protect your devices

Keep your device up-to-date with the latest security updates, and if your device can handle an upgrade from the manufacturer, go ahead and do it.



Upgrade to Windows 11 is ready—and it's free!

Get the latest version of Windows, with a new look, new features, and enhanced security.

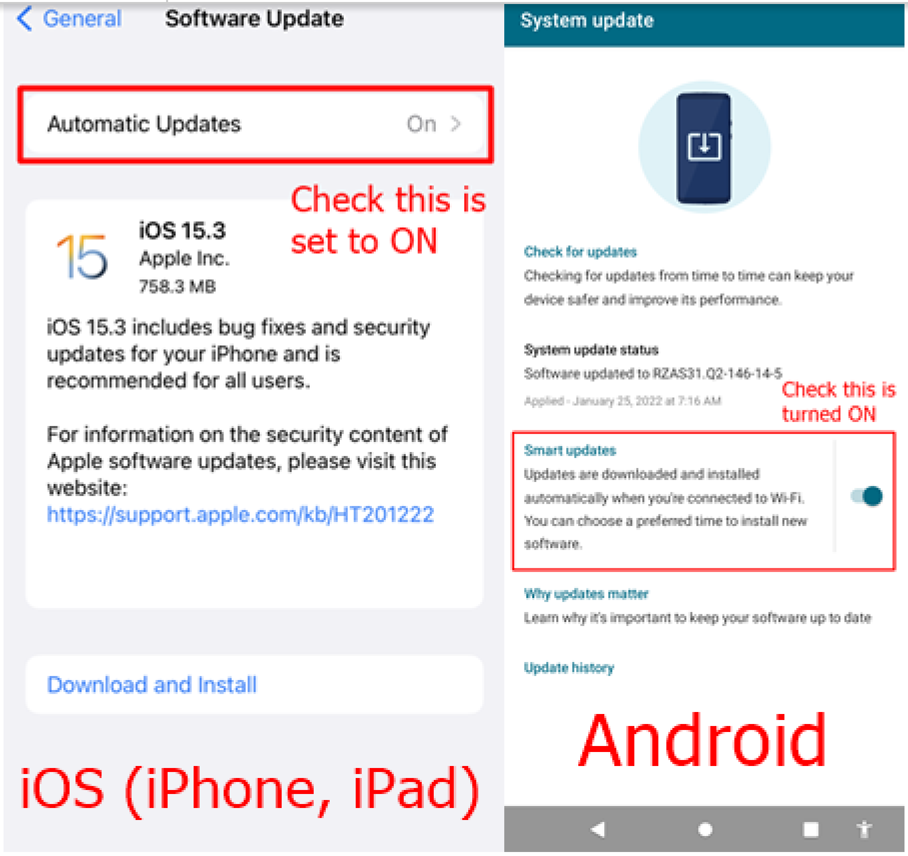
Note: Some Windows 10 features aren't available in Windows 11. Certain apps and features may have additional requirements. Check device specifications

Updates available
Last checked: Today, 7:53 AM

2021-09 Cumulative Update Preview for Windows 10 Version 21H1 for x64-based Systems (KB5005611)
Status: Pending install

Pause updates for 7 days
Visit Advanced options to change the pause period

(Note: The difference between an update and an upgrade? Updates keep your current version such as iOS 15.2 and update to 15.3. Upgrades go from macOS 10.15 to macOS 11 or Windows 10 to 11.)



Automatic Updates On >

Check this is set to ON

iOS 15.3
Apple Inc.
758.3 MB

iOS 15.3 includes bug fixes and security updates for your iPhone and is recommended for all users.

For information on the security content of Apple software updates, please visit this website: https://support.apple.com/kb/HT201222

iOS (iPhone, iPad)

Checking for updates from time to time can keep your device safer and improve its performance.

System update status
Software updated to RZAS31.Q2-146-14-5
Applied - January 25, 2022 at 7:16 AM

Check this is turned ON

Smart updates
Updates are downloaded and installed automatically when you're connected to Wi-Fi. You can choose a preferred time to install new software.

Learn why it's important to keep your software up to date

Android

- Update/upgrade (keep the device up-to-date)
  - macOS
  - Windows
  - iOS (iPhones, iPads)
  - Android

- Use security software
  - macOS
  - Windows
  - iOS (iPhone, iPad)
  - Android
  - For extra third party security, consider getting one of these security suites: PC Magazine - The Best Security Suites for 2022

Links to phishing information on company websites

- Apple - Recognize and avoid phishing messages, phony support calls, and other scams
- AOL - Identify legitimate AOL websites, requests, and communications
- Amazon - Identifying Whether an Email, Phone Call, Text Message, or Webpage is us
- eBay - Recognizing phishing phone calls and emails
- Google - Avoid and report phishing emails
- Microsoft - Protect yourself from phishing (watch the video)

- Xfinity – What is Phishing?

Links to how to protect your system on company websites

- Apple - Protecting against malware in macOS
- AOL – Protect yourself from Internet scams
- Amazon - Protect Your System
- eBay - Protect Your Information
- Google - Protect yourself from malware
- Microsoft - security help & learning
- Verizon - Hack Protection, Anti-Virus and Ad Blocker for Android and iPhone

Where to report phishing activity (help others)

- FTC - How To Recognize and Avoid Phishing Scams: Forward it to the Anti-Phishing Working Group at reportphishing@apwg.org.
- Apple – Report a problem (sign in, then select “Report a scam or fraud” from drop down list)
- Amazon - Report Something Suspicious
- eBay - If you're suspicious about an email that claims to be from eBay, sign in to My eBay and click the Messages tab. If you don't see the same message there, the email is fake. To report a fake email, forward it as an attachment to spoof@ebay.com.
- Google - Avoid and report Google scams
- Microsoft - Report a technical support scam
- Xfinity (aka Comcast): Forward the spam message as an attachment to missed-spam@comcast.net.

How to protect yourself from identity theft

- Use random and unique passwords for every account. Keep an up-to-date record of all passwords.

- Use a password manager to keep track of your random passwords (or a document or spreadsheet).
  - Dashlane, 1Password, LastPass, Norton, Google Chrome, Safari and Edge browsers, etc.
  - Password document templates: Word, Excel, PDF

- Turn on 2-step verification (aka multi/two-factor authentication, MFA, 2FA) on all accounts where available. Every company is different, so sign in to each account to look for it.
  (Note: With 2-Step Verification, if a bad guy gets a hold of your password, he will still need your phone (text message or call) or Security Key (cell phone app or device) to get into your account.). More info: The Verge - How to set up two-factor authentication on

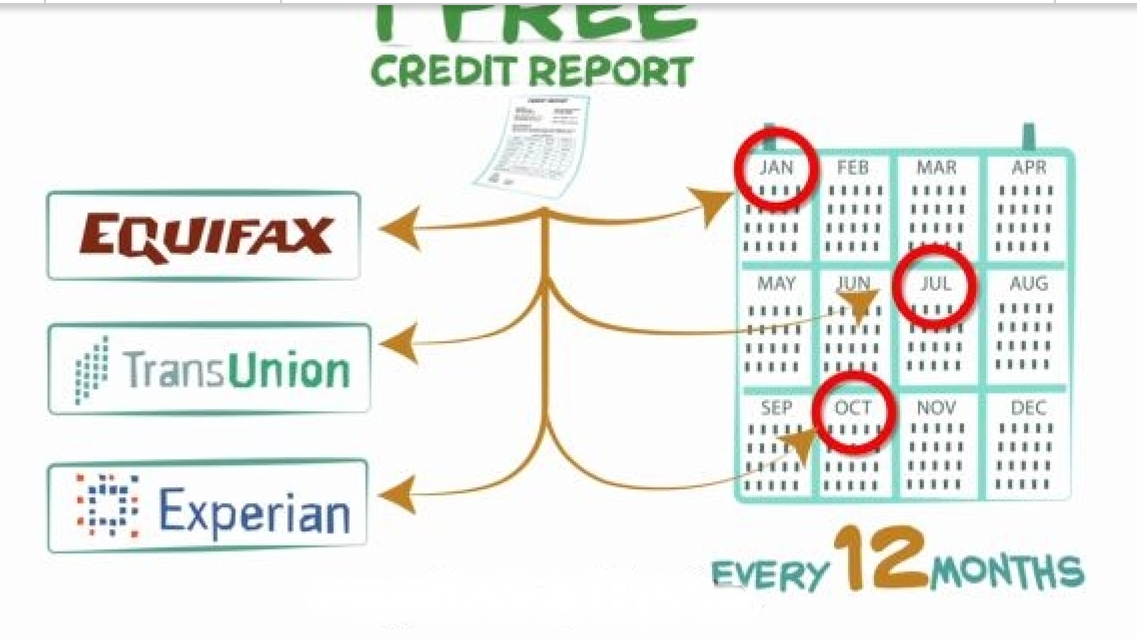
- **Freeze your credit files at:**
    - TransUnion
      P.O. Box 2000
      Chester, PA 19016-2000
      (800) 916-8800
      https://www.transunion.com/credit-freeze
      Place or lift freeze online or call 888-909-8872
      To report an inaccuracy, please visit: https://service.transunion.com

    - Experian
      P.O. Box 9701
      Allen, TX 75013-9701
      (855) 414-6047
      https://www.experian.com/freeze/center.html
      Place or lift freeze online or call 888-397-3742
      To report an inaccuracy, please visit:
      https://www.experian.com/disputes/main.html

    - Equifax
      P.O. Box 105788
      Atlanta, GA 30348
      (800) 685-1111
      https://www.equifax.com/personal/credit-report-services/credit-freeze/
      Place or lift freeze online or call 888-766-0008
      To report an inaccuracy, please visit:
      https://www.equifax.com/personal/credit-report-services/credit-dispute/

- **Freeze your National Consumer Telecom & Utilities Exchange (NCTUE) data file:**
    - Security Freeze
      Exchange Service Center – NCTUE
      P.O. Box 105561
      Atlanta, GA 30348
      https://www.nctue.com/consumers
      Place or lift freeze online: https://www.exchangeservicecenter.com/Freeze/#/
      or call 866-349-5355

- **Get an IRS Identity Protection PIN (IP PIN) so no one else can file a federal tax return in your name:** https://irs.gov/GetAnIPPIN (must get a new PIN every year before filing)



- **Get a free copy of your credit report once every 12 months from each of the 3 credit agencies at:**
    - Annual Credit Report Request Service
      P.O. Box 105281
      Atlanta, GA 30348-5281
      https://www.annualcreditreport.com
      Or call (877) 322-8228.
      Tip: Get one report from a different agency every 4 months to keep a closer watch for identity theft. More info: https://tinyurl.com/2p8stsxa.

      Note: Only one website — AnnualCreditReport.com — is authorized to fill orders for the free annual credit report you are entitled to under law.

I hope this information helps. Remember, some people say www stands for World, Wide, Web, but I say it means Wild, Wild, West, so be careful out there. Let me know if you need help with any of this and to help you get organize, here is a security checklist so you don't miss anything.

Security checklist for you and your technology

- I have an external backup drive for my computer? Yes_____ No_____ and I know how to check that it is working? Yes____ No____

    - Apple iCloud: Yes____ No____ (see what you find at https://icloud.com)
    - Microsoft OneDrive: Yes____ No____ (see what you find at https://onedrive.com)
    - Google Drive: Yes____ No____ (see what you find at https://drive.google.com)
    - Dropbox: Yes____ No____ (see what you find at https://dropbox.com)
    - Carbonite: Yes____ No____ (see what you find at https://carbonite.com)
    - Other: ______________________
    - None: ____

- My cell phone backup is turned on?
    - iOS backup (Apple): Yes____ No____
    - Android backup (Google): Yes____ No____

- My computer has all its updates/upgrades? Yes____ No____ Cell phone? Yes____ No____

- I am using security software on my computer?
    - Built-in security____
    - Norton____
    - MacAfee____
    - Other: __________________________

- I am using random/unique passwords for every account? Yes____ No____

- I have turned on 2FA/MFA on every account where available? Yes____ No____

- I am using a password manager (or document or spreadsheet)? Yes____ No___
    - Name: ____________________________

- I have frozen my credit files?
    - TransUnion: Yes____ No____
    - Experian: Yes____ No____
    - Equifax: Yes____ No____
    - National Consumer Telecom & Utilities Exchange (NCTUE): Yes____ No____

- I have an IRS Identity Protection PIN (IP PIN)? Yes____ No____

- I am getting a free credit report once every 4 months from TransUnion, Experian, Equifax? Yes____ No____

  Security Checklist PDF version or DOC version

More Info:

Please watch this 2 minute video: Microsoft - Protect yourself from tech support scams

FTC - Want to know who stole your identity? Getting your records can help.

FTC - Did you get an email saying your personal info is for sale on the dark web?

FTC - What to do about unwanted calls, emails, and text messages that can be annoying, might be illegal, and are probably scams.

Mailxaminer - Learn How To Identify Fake Emails To Spot Fraud?

The Verge - How to set up two-factor authentication on your online accounts

Microsoft - Breaking down a notably sophisticated tech support scam M.O.

Nerdwallet - How to Freeze Your Credit

What is the process to place a security freeze on my NCTUE reports?

2020 Colorado Revised Statutes Title 5 - Consumer Credit Code cle 18. Colorado Consumer Credit Reporting ActArti Section 5-18-106. Disclosures to consumers.

Copyright © 2022 Kerno.biz LLC, All rights reserved.

Want to change how you receive these emails?
You can update your preferences or unsubscribe from this list.

mailchimp