How to keep yourself safe on line

A guide for on line safety

March 2022

Types of threats

- Spam - unwanted messages
- Phishing - fake messages designed to capture personal information
- Hacks - Breaking into your accounts
- Scams - ways to get you to transfer money to scammers
- Malware - Software designed to disrupt, damage, or gain unauthorized access to a computer system.
- Ransomware - Computer is taken over and ransom paid to unlock your data

Definitions

- Cookies - Data from your browsing history that stays on your computer. You can tailor these to prevent sale of your data or tracking for advertising.
- VPN - Virtual Private network
- IP (Internet Protocol) Address - every device has one. Assigned by Internet Service Provider
- ISP - Internet Service Provider

What you can do to stay safe on-line

- Strong passwords
- Be careful with e-mail
- Two factor authentication
- Anti-virus protection
- Keep your software updated
- Clear your cache (history of sites you have visited)
- Beware of public wifi (Starbucks, McDonald’s, etc.)
- Back up your data

Rule 1: Strong Passwords

- Use alphanumeric, capital letter plus a symbol
  - Capital Letter(s), number and symbol !#$
  - Ten characters or more
  - Something that is easy to remember: *Ihavebut1life2give#*
  - Different passwords for each account
  - Change passwords periodically (every three months)
  - Some browsers create complex passwords for you
  - Use a password manager

Rule 1: Strong Passwords

Password Managers

- A Password Manager creates strong passwords for your accounts
- You only need to remember one password
- Some browsers have their own password managers
  - Limited in functionality but easier to use
    - Apple iCloud keychain
    - Google Password Manager
    - Firefox Lockwise

Rule 1: Strong Passwords

Password Managers

- Third Party Password Managers
  - Dashlane (free or pay)
  - Lastpass Premium
  - 1Password
  - Bitwarden (free, mostly)
- Take some setup
- Have extra features to help with account security

Rule 2: Be careful with e-mail

- Only from people you know
  - Even then be careful
  - Suspicious e-mails
- Fake invoice e-mails
- What to watch out for:
  - Items you didn’t order (Norton Anti-virus protection)
  - Odd requests from people you know (gift cards, money, etc.)
  - Poor grammar and spelling in messages
  - Wrong e-mail addresses
- What to do?
  - Report spam or scam messages
  - Tag e-mail as spam or phishing

Fraudulet e-mail

BILL No. UOK01142022YM Inbox ×

jaoh oowh <cjaohoowh687@gmail.com>
o nortoncc2021, bcc: me

Dear Buyer,

Your Yearly subscription for NORTON TOTAL PROTECTION has been renewed AND updated successfully.
==========

The charged amount will be reflected within the next 24 to 48 hrs on your profile of account.

PRODUCT DETAILS

._____===_____+

NVOICE NO. @ **UOK01142022YM**
Product Title @ **NORTON TOTAL PROTECTION**

._____+
START DATE @ **2022-01-14**
End Date @ **1 year from Start Date**

._____=====_____+
Total @ **$236.87 USD**
Method of Payment @ **Automatic Debit**

._____====_____+

f you wish to stop subscription and claim a **REFUND** then please feel free to call our Billing Dept. as soon as possible.

You can Reach us on : **+1 – (803) – (-82) – 0-65**

Rule 3: Two Factor Authentication

1. Two steps to get on line:
    - Enter your password
    - You get a text on your phone or an e-mail with a code you enter
2. Enable it wherever possible

Rule 4: Anti-virus protection

- Windows and Apple PCs come with some level of anti-virus
  - Better than nothing, but a commercial product is better
- Anti-virus can help protect against phishing, malware and ransomware
- Bitdefender, Norton Anti-virus, McAfee, Kapersky. Yearly subscription price, first year discounts available.

Rule 5: Download Security Updates regularly

- Protects your devices from latest security threats

Rule 6: Check your data breach status

- Has your personal information been compromised?
- https://haveibeenpwned.com

Rule 7: Clear your computer cache

- Delete browser cookies and clear your browser history regularly.
  - Frees up disk space
  - Speeds up browsing

Rule 8: Be careful with public wifi

https://1password.com/downloads/#browsers

- Use a VPN if you use public wifi often
- Fairly inexpensive - $3-5/month
- You have no idea how secure public wifi is?
- Someone else on the network could get into you computer
- A VPN
  - Hides your IP address
  - Encrypts your internet traffic

Rule 9: Back up your data

- Back up your data
  - To the cloud
  - Your own backup disk

Sources

- https://www.washingtonpost.com/technology/2021/12/16/secure-password-guide/
- https://www.wsj.com/articles/the-best-password-managers-and-security-tips-how-to-solve-your-login-problems-11615122001?mod=article_inline
- https://www.wsj.com/articles/how-google-and-apples-free-password-managers-compare-with-1password-dashlane-and-others-11626012003
- https://www.pcmag.com/picks/the-best-free-antivirus-protection
- https://www.pcmag.com/how-to/12-simple-things-you-can-do-to-be-more-secure-online
- https://www.pcmag.com/picks/the-best-free-password-managers
- https://www.pcmag.com/picks/the-best-antivirus-protection
- https://www.npr.org/2020/10/09/922262686/your-technology-is-tracking-you-take-these-steps-for-better-online-privacy
- https://www.consumerreports.org/products/password-managers-200399/password-managers-200401/recommended/
- https://us.norton.com/internetsecurity-privacy-should-you-delete-cookies.html