

Be Engaged. Be Informed. Be Heard.



HOMEOWNERS ASSOCIATION
OF TELlico VILLAGE, INC

Your Voice in the Village



Cyber Security – Part 1

Protecting Your Personal Communications

Additional Information & Links

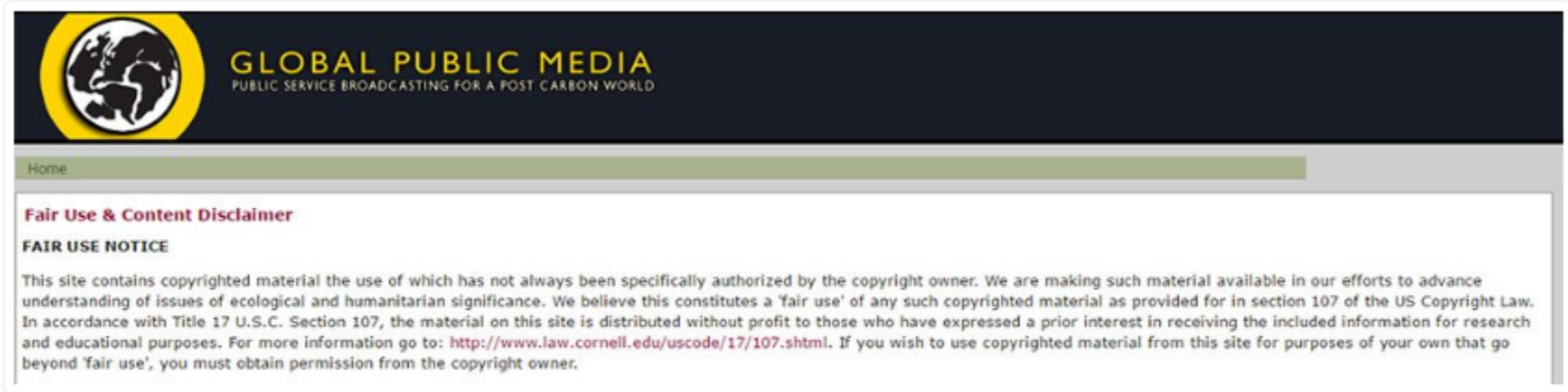
Joint Education Presentation by

Tellico Village 
**COMPUTER
USERS CLUB**


HOMEOWNERS ASSOCIATION
OF TELLICO VILLAGE, INC

Disclaimer:

HOA and/or TVCC is not responsible for any errors or omissions, or for the results obtained from the use of this information. All information in this site is provided “as is”, with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this information...”



The image shows a screenshot of a website header and a disclaimer section. The header features a logo on the left consisting of a yellow circle with a black and white globe inside. To the right of the logo, the text reads "GLOBAL PUBLIC MEDIA" in yellow, with "PUBLIC SERVICE BROADCASTING FOR A POST CARBON WORLD" in smaller white text below it. Below the header is a green navigation bar with the word "Home" in white. The main content area has a red heading "Fair Use & Content Disclaimer" and a bold sub-heading "FAIR USE NOTICE". The text below the sub-heading reads: "This site contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available in our efforts to advance understanding of issues of ecological and humanitarian significance. We believe this constitutes a 'fair use' of any such copyrighted material as provided for in section 107 of the US Copyright Law. In accordance with Title 17 U.S.C. Section 107, the material on this site is distributed without profit to those who have expressed a prior interest in receiving the included information for research and educational purposes. For more information go to: <http://www.law.cornell.edu/uscode/17/107.shtml>. If you wish to use copyrighted material from this site for purposes of your own that go beyond 'fair use', you must obtain permission from the copyright owner."

Mass Equality has a “Fair Use Policy” and “Legal Disclaimer” that includes the same standard notice:

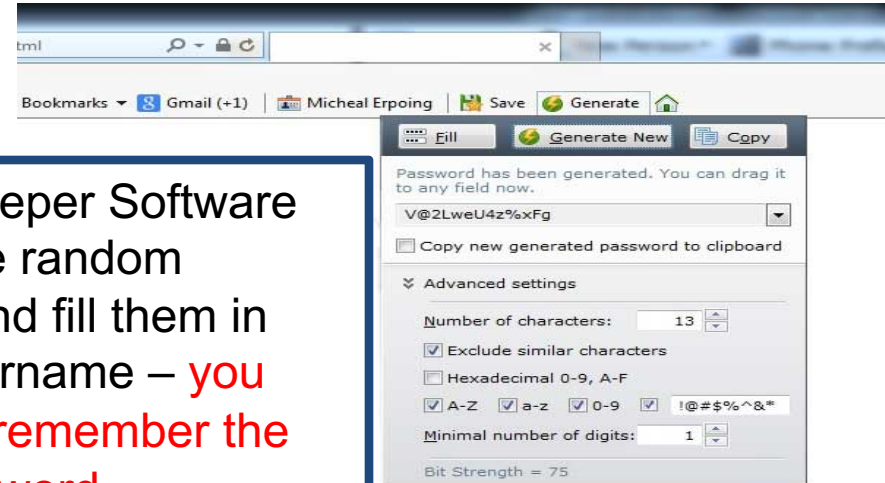
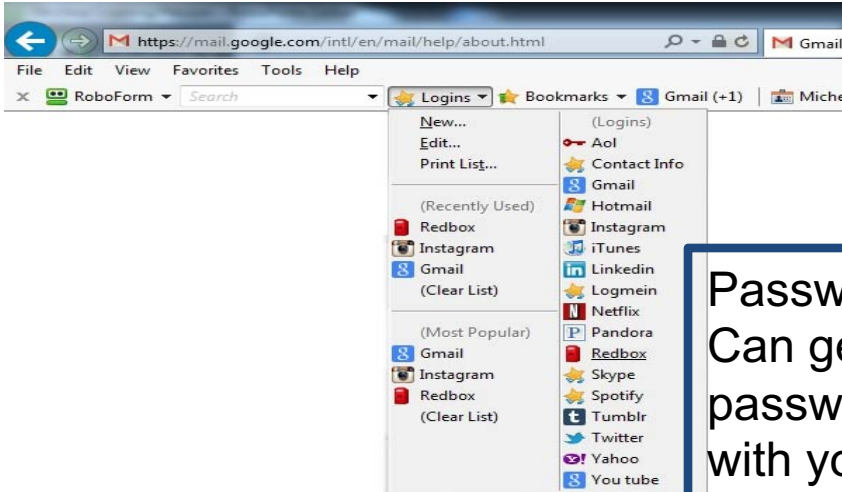
Contents

- **Password Keepers –**
 - What they are and How to Use
 - Screenshots & links to Paid For & Free Password Keepers
- **SHUT YOUR PHONE DOWN COMPLETELY AND WAIT FOR AT LEAST 30 SECONDS TO RE-BOOT.**
- **DO NOT JUST DO A “RESTART” – THIS DOES NOT COMPLETELY CLEAR THE MEMORY.**
- Use many of the same types of protective programs and cautions as a computer to shield you.
- **Process Updates as soon as available!!!!!!**

Password Keepers

Never Forget or Have to Remember Passwords Again

We hate remembering passwords. Storing your passwords on paper, in a spreadsheet or in your browser is vulnerable to cyber criminals. With Keeper, you'll never have to remember passwords again. Keeper stores and manages your passwords in your Keeper vault.



Password Keeper Software
Can generate random
passwords and fill them in
with your username – you
only need to remember the
Master Password

Quick How to Create and Use a Password with a Password Manager

The screenshot shows the Kohl's website's account creation page. The browser address bar displays 'https://www.kohls.com/myaccount/kohls_login.jsp?action=createAccount'. The page header includes the Kohl's logo, a search bar, and navigation links for Account, Shopping Cart (\$0.00), and Check Out. Below the header, there are links for 'Shop by Department', 'My Store: Bucktown', 'Kohl's Coupons', and 'Help'. The main content area is titled 'Create Account' and contains the following fields and options:

- First Name:** John
- Last Name:** Doe
- Email Address:** J.Doe@yahoo.com
- Password:** (field with a 'Show password' link and a note: 'Should not be same as email or login')

Below the form, there are options for 'YES2YOU REWARDS' (I signed up in store, Enroll Today!, No Thanks) and a checkbox for 'Yes, sign me up!' to receive e-mail offers. At the bottom of the form are 'CREATE ACCOUNT' and 'CANCEL' buttons, and a 'BACK TO TOP' link.

Red arrows from the text box on the right point to the 'Last Name' and 'Email Address' fields.

Go to a Site,
Like Kohl's,
And enter your
User Name & email
address

John Doe
J.Doe@yahoo.com

We'll generate the
Password next

Generate and add Password

The screenshot shows the Kohl's account creation page. The browser address bar displays `https://www.kohls.com/myaccount/kohls_login.jsp?action=createAccount`. The page header includes promotional banners for shipping and pickup, and navigation links for Account, Cart, and Checkout. The main content area is titled "Create Account" and contains fields for First Name (John), Last Name (Doe), Email Address (J.Doe@yahoo.com), and Password. A "Show password" link is next to the password field. A RoboForm password manager overlay is active, showing a generated password "K@X@n8YAC^Fy52" and a "Generate" button. A red arrow points from the "Generate" button to the "Generate" button in the RoboForm overlay. Another red arrow points from the "Show password" link to the password field. A third red arrow points from the "Generate" button in the RoboForm overlay to the password field. The RoboForm overlay also includes a "Copy" button and a "Security Center" link.

Select Password Manager

From the Drop-down Select: "Generate"

Cut and Paste the Generated Password

This time it is:

K@X@n8YAC^Fy52

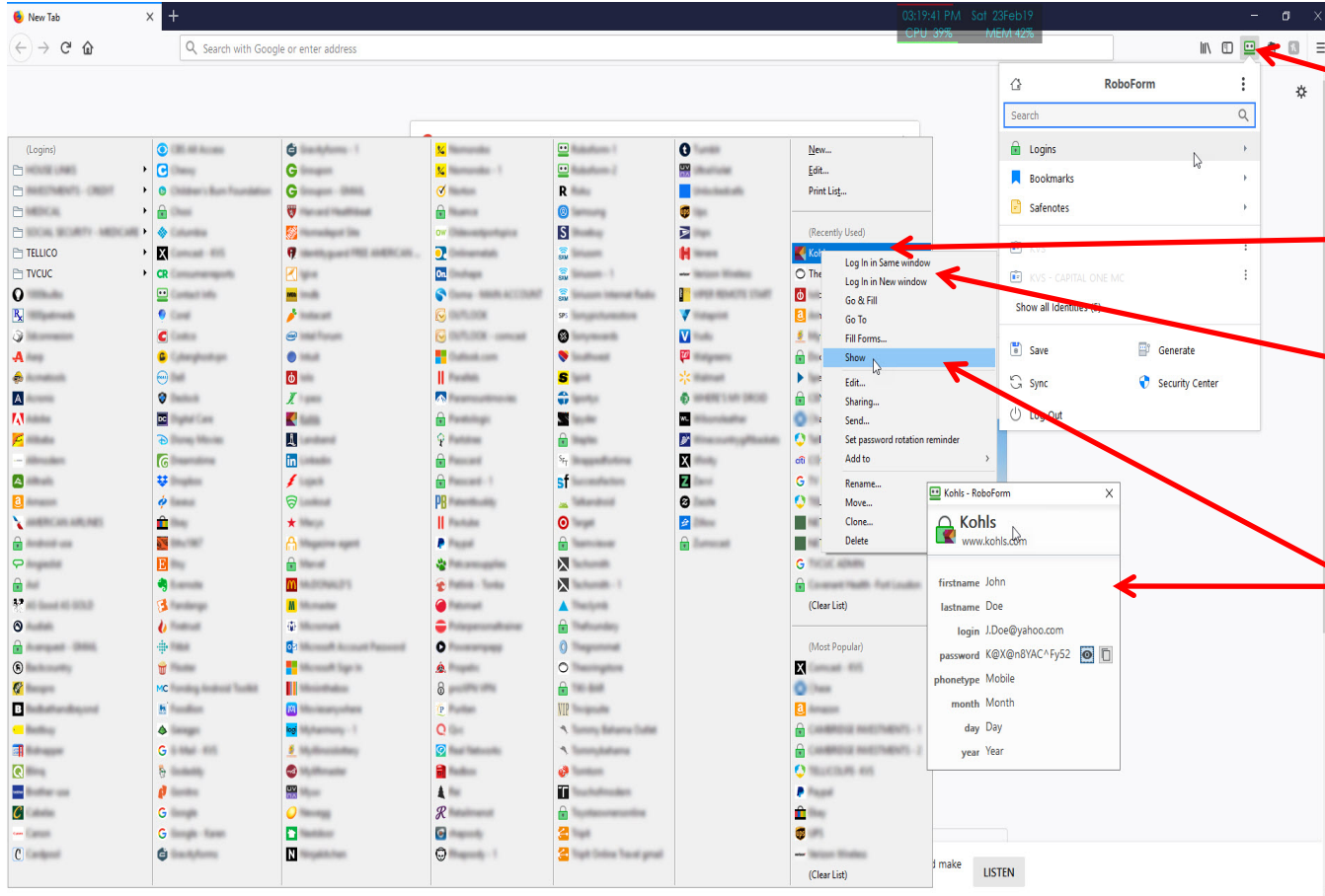
14 characters – it can Generate longer ones

Create the Account and Save the Logon Credentials

The screenshot shows the Kohls.com account page. The browser address bar displays 'https://www.kohls.com/myaccount/v2/myinfo.jsp'. The page header includes promotional text: 'FREE shipping with \$75 purchase details FREE store pickup today EXTRA 20% OFF use SNOWDAY20 get your pass'. The main navigation bar features the Kohls logo, a search bar with the text 'Hi John, what are you looking for today?', and user account information for 'John' with a '\$0.00' cart and a 'Check Out' button. Below the navigation bar, there are links for 'Shop by Department', 'My Store: Farragut', 'Kohl's Coupons', and 'Help'. The main content area is divided into a left sidebar and a main panel. The sidebar contains links for 'Hi John!', 'My info', 'About Me', 'Address Book', 'Billing & Payment Info', 'Communication Preferences', 'Orders', and 'Yes2You Rewards'. The main panel displays account details for 'John Doe' (j.doe@yahoo.com) under the 'About Me' section, a masked 'Account Password' field, and an 'Annual Gross Income (optional)' field. A RoboForm password manager overlay is visible on the right side of the page, asking 'Do you want RoboForm to save your password?'. The overlay shows the 'Name' as 'Kohls' and the 'Folder' as 'Home'. There are three buttons at the bottom: 'Never for this site', 'Cancel', and 'Save'. Two red arrows point from the 'Save' button to the text box on the right.

Click on "Save"
And which folder
to put it in if you
use folders to
organize

You are now able to Just “Click & Go”



1: Select Password Manager

2: Select “Kohls”

3: Select “Existing Window or “New Window”

Highlighted “Show” Shows what will be filled in.

Existing Accounts or Changing Password

- To add an existing account, go to that site and logon as usual, just click “SAVE” in the Password Manager and that will be added. Over time you will have them all in.
- If you have to change your password, just click “SAVE” in the Password Manager and choose to overwrite the existing or a new “XXXXXX-X” (Kohl’s-1) selection.

You can create the new password using “Generate”.

- Password Managers make keeping your passwords ready to use and update. No more searching for that lost scrap of paper, or finding a bunch for the same site and wondering which is right. Other information can be safely kept like a note with Serial Keys for Windows or other programs.
- If you use a paid version, you can have your Computer and Smart Phone Linked to get the information if your Computer is locked. You can share the same logons by using the same Password Manager credentials.

The Key is to create a very strong password for the Manager, to keep everything safe. It is the only one you need to remember.

Product	Zoho Vault	Dashlane	Sticky Password Premium	Keeper Password Manager & Digital Vault	LastPass Premium	Password Boss Premium v2.0	LogMeOnce Password Management Suite Ultimate	RoboForm 8 Everywhere	AgileBits 1Password	True Key by Intel Security
Lowest Price	\$12.00 Zoho	\$39.99 Dashlane - Synced	\$14.99 Special Offer	\$25.49 Keeper Security	\$24.00 LastPass	\$29.00 Password Boss	\$39.00 MSRP	\$19.95 RoboForm	\$35.88 MSRP	\$19.99 MSRP
	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT		SEE IT		
Editors' Rating	●●●●○	●●●●● EDITORS' CHOICE	●●●●○	●●●●● EDITORS' CHOICE	●●●●○	●●●●○	●●●●○	●●●●○	●●●●○	●●●●○
Import From Browsers	—	✓	✓	✓	✓	✓	✓	✓	✓	✓
Two-Factor Authentication	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Fill Web Forms	—	✓	✓	✓	✓	✓	✓	✓	✓	—
Multiple Form-Filling Identities	—	✓	✓	✓	✓	✓	✓	✓	✓	—
Actionable Password Strength Report	✓	✓	—	✓	✓	✓	✓	✓	✓	—





#AmazonHQ2

#Mars

#GPSFail

#GalaxyS10

#TeslaDogMode

Subscribe:  

Reviews | Software | Security | Password Managers

The Best Free Password Managers for 2019

A password like '123456' may be easy to remember, but it's also equally easy to guess or hack. These are the best free password managers that can help you keep track of strong, unique passwords for every secure site you use.



By Neil J. Rubenking February 15, 2019 10:29AM EST


















 74 SHARES

PCMag reviews products independently, but we may earn affiliate commissions from buying links on this page. [Terms of use.](#)

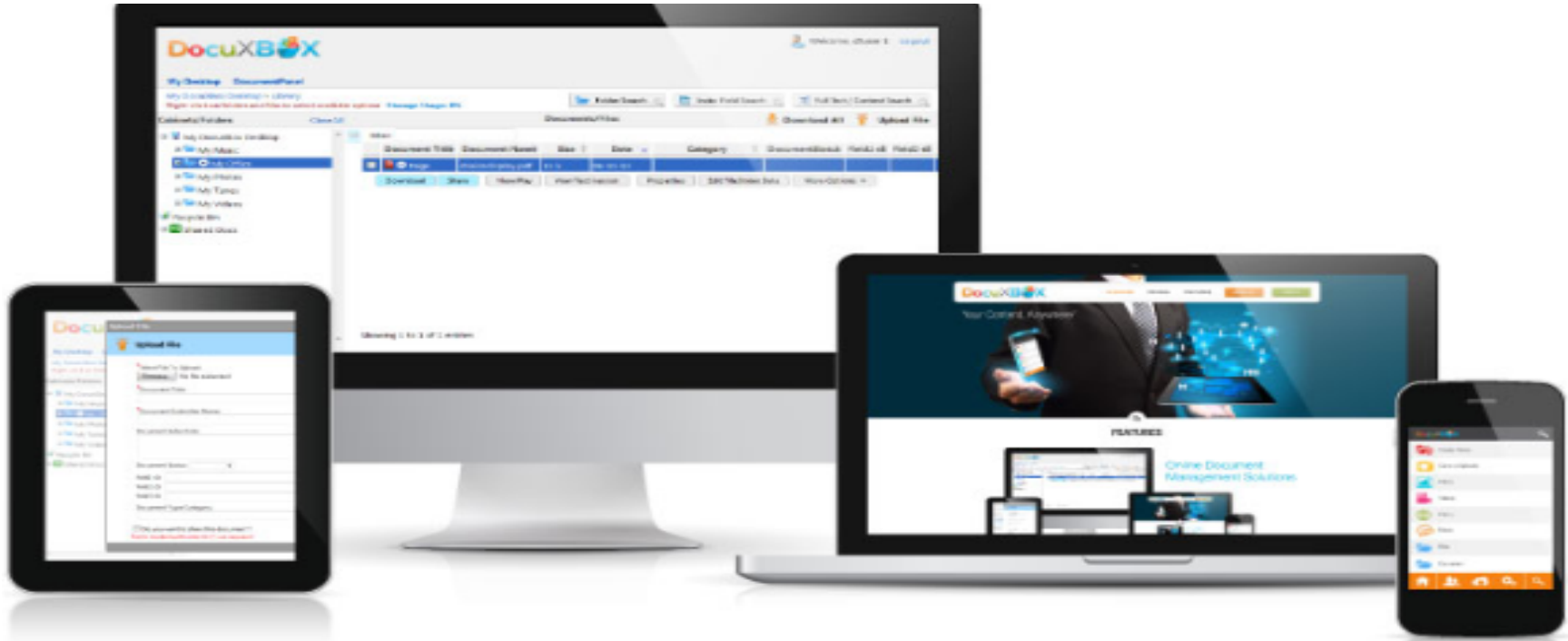
Product	LastPass	Myki Password Manager & Authenticator	LogMeOnce Password Management Suite Premium	1U Password Manager	Avira Password Manager	Enpass Password Manager	KeePass 2.34	oneID	Symantec Norton Password Manager
									
	Free	\$0.00	Free	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00

<https://www.pcmag.com/roundup/331555/the-best-free-password-managers>

So Now We'll Ask the Question: How **Should** You Protect Yourself?

- #1 Use Strong Passwords – REAL ONES!! – Keep updated.
- Have a safe strategy for keeping Passwords.
- Consider Password Keeper Software.

Are Any Devices “Safer” than Others?



No, not really, it is most often us who let the hacker in

COMPUTER THREAT – YES, EVEN APPLE PRODUCTS

CAN BE ATTACKED

- If you get a message that your computer has been attacked and you have only a few seconds to respond to a phone number to fix it:

**SHUT YOUR COMPUTER DOWN COMPLETELY AND WAIT FOR AT LEAST 30 SECONDS TO RE-BOOT.
DO NOT JUST DO A “RESTART” – THIS DOES NOT COMPLETELY CLEAR THE MEMORY.**

Fear blocks reason. The goal is to frighten you enough to stop you from thinking clearly.

- These messages frighten people into letting strangers take control of your computer and charge you to fix them, allowing them to lock you out or steal information – and your money. Most likely your computer will be trashed.
- Install, keep updated and use Anti-Virus programs. Yes, you can get some for free, but consider the benefits of a subscription and if it offers more protection.
- Install, keep updated and use Malware programs. Yes, you can get some for free, but consider the benefits of a subscription and if it offers more protection.
- Install, keep updated and use Anti-Ransom Ware programs. You can get some for free, some are being included in Anti-Virus programs as part of a subscription.

<https://www.wcpo.com/money/consumer/dont-waste-your-money/listen-new-talking-tech-scam-takes-over-your-pc>

SMART PHONE THREATS

- **A Smart Phone is a computer.** Messages or links like those sent to a computer will pop up and cannot be dismissed.
- **SHUT YOUR PHONE DOWN COMPLETELY AND WAIT FOR AT LEAST 30 SECONDS TO RE-BOOT.**
- **DO NOT JUST DO A “RESTART” – THIS DOES NOT COMPLETELY CLEAR THE MEMORY.**
- Use many of the same types of protective programs and cautions as a computer to shield you.
- **Process Updates as soon as available!!!!!!**

Settings to Secure Your iPhone, iPad

- 1. Turn on USB Restricted Mode to make hacking more difficult**
- 2. Make sure automatic iOS updates are turned on**
- 3. Set a stronger device passcode**
- 4. Switch on two-factor authentication**
- 5. Change your reused passwords**

iOS 12's password manager has a new feature: password auditing. If it finds you've used the same password on multiple sites, it will warn you and advise you to change those passwords. It prevents password reuse attacks (known as "[credential stuffing](#)") that hackers use to break into multiple sites and services using the same username and password.

Ways to Secure Android Phones

- 1. Only buy smartphones from vendors who release Android patches quickly.**
- 2. Lock your phone.**
- 3. Use two-factor authentication.**
- 4. Only use apps from the Google Play Store.**
- 5. Use device encryption.**
- 6. Use a Virtual Private Network.**
- 7. Turn off connections when you don't need them.**
- 8. If you don't use an app, uninstall it.**

How many have heard of Cryptojacking??

- Cryptojacking is defined as the secret use of your computing device to mine cryptocurrency. It is a Hijacking of your machine.
- **How does in-browser cryptojacking work?**
- In-browser cryptojacking uses JavaScript on a web page to mine for cryptocurrencies.
- JavaScript runs on just about every website you visit, so the JavaScript code responsible for in-browser mining doesn't need to be installed.
- You load the page, and the in-browser mining code just runs. No need to install, and no need to opt-in.
- It generally causes no “damage” to your machine – it just runs in the background using your machine to help steal from other sites.
- [Cryptojacking blocker](#)
- The simplest way to protect yourself from cryptojacking is to install a cryptojacking blocker.

<https://hackerbits.com/programming/what-is-cryptojacking/>

<https://www.csoonline.com/article/3253572/internet/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html>

Ransomware - Malware

HYDRACRYPT

All Your files and documents were encrypted!
ID : [REDACTED]

Encryption was made with a special crypto-code!
There NO CHANCE to decrypt it without our special software and your unique private key!

To buy your software You need to contact us by EMAIL:
1) XHELPER@DR.COM
or
2) AHELPER@DR.COM
Your email text should contain your unique ID number and one of your encrypted file.

We will decrypt one of your file for FREE! It's your guarantee!
Remember! Your time has a limit: 72 hour.
If You will not send any email We will turn on a sanctions:

- 1) Your software's price will be higher
- 2) Your unique private key will be destroyed (After that your files will stay encrypted forever)
- 3) Your private info, files, documents will be sold on the Dark Markets

Attention: all your attempts to decrypt your PC without our software can destroy or damage your files!

<https://www.us-cert.gov/Ransomware>

Ransomware

- For more long-term prevention of ransomware attacks, follow these ransomware tips for businesses and consumers:
- **New ransomware variants appear on a regular basis.** Always keep your security software up to date to protect yourself against them.
- **Keep your operating system and other software updated.** Software updates will frequently include patches for newly discovered security vulnerabilities that could be exploited by ransomware attackers.
- **Email is one of the main infection methods.** Be wary of unexpected emails, especially if they contain links and/or attachments.
- **Be especially wary of any Microsoft Office email attachment that advises you to enable macros to view its content.** Unless you are absolutely sure that this is a genuine email from a trusted source, do not enable macros and instead immediately delete the email.
- **Backing up important data is the single most effective way of combating ransomware infection.** **Attackers** have leverage over their victims by encrypting valuable files and leaving them inaccessible. If the victim has backup copies, they can restore their files once the infection has been cleaned up. However, organizations should ensure that backups are appropriately protected or stored offline so that attackers can't delete them.
- **Using cloud services could help mitigate ransomware infection,** since many retain previous versions of files, allowing you to “roll back” to the unencrypted form.

<https://us.norton.com/internetsecurity-malware-ransomware-5-dos-and-donts.html>

The Dark Web

- **The Web or Internet** most everyone uses is an open, easily searched network of people, places and information. We just “Google” it, and there, whatever we want is on our screen.
- **The “Deep Web”** is special part of the internet that businesses like Banks, PayPal, Social Security, and government use to transact business and only by knowing some exact address can someone access those who use it. A “Google” search won’t find anything.
- **The “Dark Web”** is like the “Deep Web” in that special software is needed to gain access, but unlike the “Deep Web” it is filled with hackers and thieves. They set up shop like an open air Bazaar selling your full ID (SSN, mother’s maiden name, full history) for as low as: **\$2.95** Your whole life is worth \$2.95. (bitcoin – no traceable dollars) Guns, drugs, children, you name it - all for sale in the Dark Web.

The Dark Web & Basic Safeguards

- **Freeze your Credit Bureaus** so no new credit can be opened without you knowing. This also limits credit checks. This puts YOU in control.
- **Monitor ALL your accounts** so you know when and what transactions are taking place. This puts YOU in control.
- **Use a Password Manager** this is the easiest way to create a unique, random password for each site. If someone does get a password, it will only be to a single site. This puts YOU in control.

Tips for Securing Your Wireless Home Network

- **Refrain from giving out your network password.** Sign in guests yourself –or- setup GUEST network.
- **Place your router in the middle of your home.**
- **Disconnect the router when it's not in use.**
- **Use a boring network name.**
- **Consider Disabling your computer's network sharing.**

- **[Use a VPN.](#)**

- **[Replace your router.](#)**

Ken Litke comments: use this slide but use the following slide for the talking points...can put these Notes for the meeting.

Tips for Securing Your Wireless Home Network

- **Refrain from giving out the network password.** As paranoid as it may make you seem, refusing to give out your network's password lowers the chances of people who you don't trust finding out your network's password. Instead of giving out the password, offer to sign in friends and family when they visit rather than allowing them to sign into the Wi-Fi themselves.
- **Place your router in the middle of your home.** In addition to making your router coverage more balanced, doing this will limit the router's reach beyond your home's walls. This means that would-be network intruders won't be able to sit outside of your home and still connect to the network.^[1] Your home's size and layout may make this impossible; if so, just try to keep your router well-away from windows and external doorways.
- **Disconnect the router when it's not in use.** If you plan on leaving your home for a weekend or more, unplug your router and/or modem. This is more of a safety precaution than an active security measure, but it will prevent any potential attackers from connecting to your Internet while you're powerless to stop it. Even if you're going to be gone for a standard 8- or 9-hour work day, disconnecting your router will prevent any chances of your network being compromised while you're gone.
- **Use a boring network name.** It may sound stupid, but changing your clever Wi-Fi network name to a boring one will decrease the odds of it being picked out as a potential target.^[2] For example, using the router's manufacturer and its number (e.g., "Belkin-3030") as the name will make the network stand out less than if its name is "Bill Wi the Science Fi" or something similar.
- **Disable your computer's network sharing.** Network sharing allows your computer to share files and information with other computers on the network, but it also makes your computer a weak point in the network's security.
- **Use a VPN.** Virtual Private Networks, or VPNs, direct your network traffic through one or more abnormal servers, hiding your network's activity in the process. VPNs don't necessarily secure your network so much as they hide it, but that's usually enough to prevent attacks as well as reduce the likelihood of future attacks.
- **Replace your router when it becomes obsolete.** As with any technology, routers lose their value after a few years, especially in the security department. Since online threats are constantly updating and evolving, a brand-new router will be much better equipped for security than will a three- or four-year-old one.

192.168.1.1/ui/1.0.99.186168/dynamic/login.html

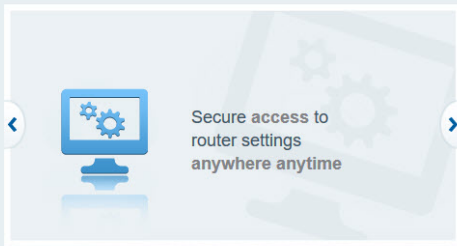
Open Browser
In URL Window

Typical Router Access Is:

192.168.1.1

Sign In

Log in with your router password.



Secure access to
router settings
anywhere anytime

Access Router

Router Password

[Show hint](#)

Sign In

English (United States)

To login with your Linksys Smart Wi-Fi account, [click here](#).

Enter Password

Your Network Control Counsel

See what is connected & to which Network

Select to setup or Change Guest Access

192.168.1.1/ui/1.0.99.186168/dynamic/home.html

LINKSYS Smart Wi-Fi

App Center Help Settings Sign Out

WRT3200ACM

Linksys Home Networking

Learn more about apps for Linksys Smart Wi-Fi Routers

Network Status

Connected

THIS DEVICE ROUTER INTERNET

Wi-Fi Settings

2.4 GHz 5 GHz

Guest Access

Guest Network is ON:

2.4 GHz SSID: 5 GHz SSID: Password: Currently: 0 guests

Network Map

Online devices:

Local	11	2.4 GHz	7
		5 GHz	2

+ Add a Device

Parental Controls

Parental Controls are OFF:

Controlled devices: None

External Storage

There is no drive in the external port.

Refresh

Media Prioritization

High Priority	
ROKU - FAMILY ROOM	Edit
Bad-Dog-1	

End User License Agreement | Privacy Statement | Third Party Licenses | Cookie Privacy Policy

© 2017 Belkin International, Inc. and/or its affiliates. All rights reserved.

Guest Access is set to "ON" or "OFF"

Edit to Add Guest Network Credentials

1st: Select "Edit"

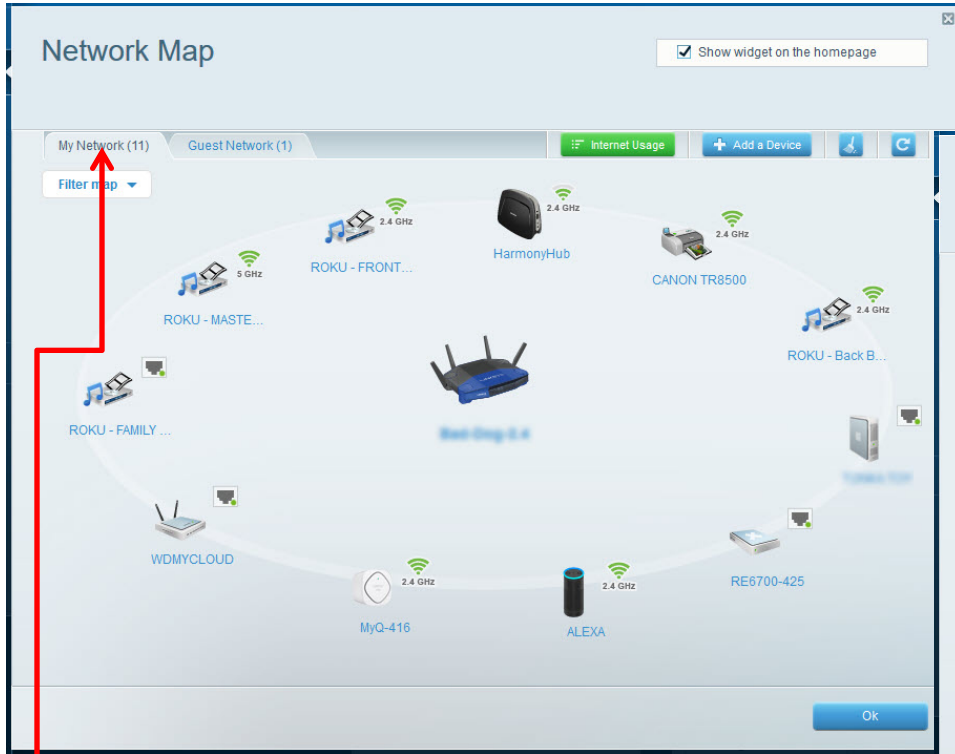
**2nd: Linksys-2.4-Guest
Linksys-5-Guest**

**3rd: Password:
YRU_\$till_H@r@
(Why Are You Still Here)**

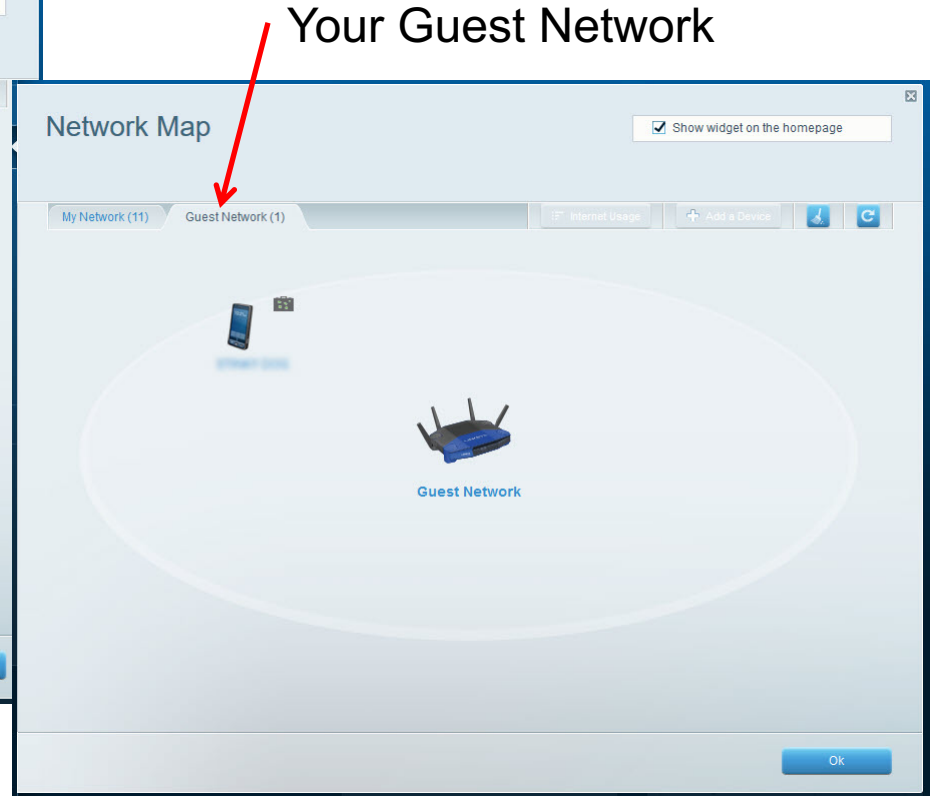
Lastly, click to "ON" then "OK"
Exit Router choosing "Save Changes"

The screenshots show the 'Guest Access' configuration page. The first screenshot shows the 'Edit' link next to the 'Guest network names and password' section. The second screenshot shows the 'Allow guest access' toggle set to 'OFF', and the 'Guest network names and password' section with the 2.4 GHz SSID set to 'Linksys-2.4 - Guest', the 5 GHz SSID set to 'Linksys - 5 - Guest', and the password set to 'YRU_\$till_H@r@'. The third screenshot shows the 'Allow guest access' toggle set to 'ON' and the 'OK' button highlighted.

Use "Network Map" to see Your Networks



Your Private Network



Your Guest Network

Virtual Private Network

- Consider using a VPN (Virtual Private Network) which masks your computer's address and creates an encrypted "Tunnel" in the internet between your computer and where you are connecting to shield you from hackers.
- There is a subscription fee to cover the cost of all the servers used and there is a bit of slowing.

Some VPNs (CNET)

- NordVPN – 5 / 5 - best plan is [1-year subscription plan: \\$6.99 \(\\$83.88\)](#). While their monthly price of [\\$11.95](#), their yearly price of [\\$83.88](#)
- STRONGVPN – 5 / 5 - [monthly price of \\$10](#) is in the middle of the pack, but their yearly price of \$69.99
- IPVanish VPN – 4.5 / 5 - [\\$7.50/month](#) and [\\$58.49 for a year](#),
- PureVPN – 4.5 / 5 - Pricing is middle-of-the-road, at [\\$10.95 per month](#) and [\\$69.00 for three year's service](#).
- ExpressVPN – 4 / 5 - [Their best plan is priced at just \\$6.67](#) per month for an annual package which includes 3 extra months free.
- Buffered VPN – 4/5 At [\\$12.99](#) per month and [\\$99.00](#) for a year of service
- Goose VPN – 4.5 / 5. monthly fee for unlimited bandwidth is a middle-of-the-road \$12.99/month, but if you spend \$59.88 for a year's service,
- <https://www.cnet.com/best-vpn-services-directory/>

What is "https" and Why Do I care?



https

The screenshot shows the American Express website interface. At the top, the browser's address bar displays the URL `https://www.americanexpress.com`. Below the address bar, there are navigation links for "My Account", "Cards", "Travel", "Rewards", and "Business". A login form is overlaid on the page, containing the following elements:

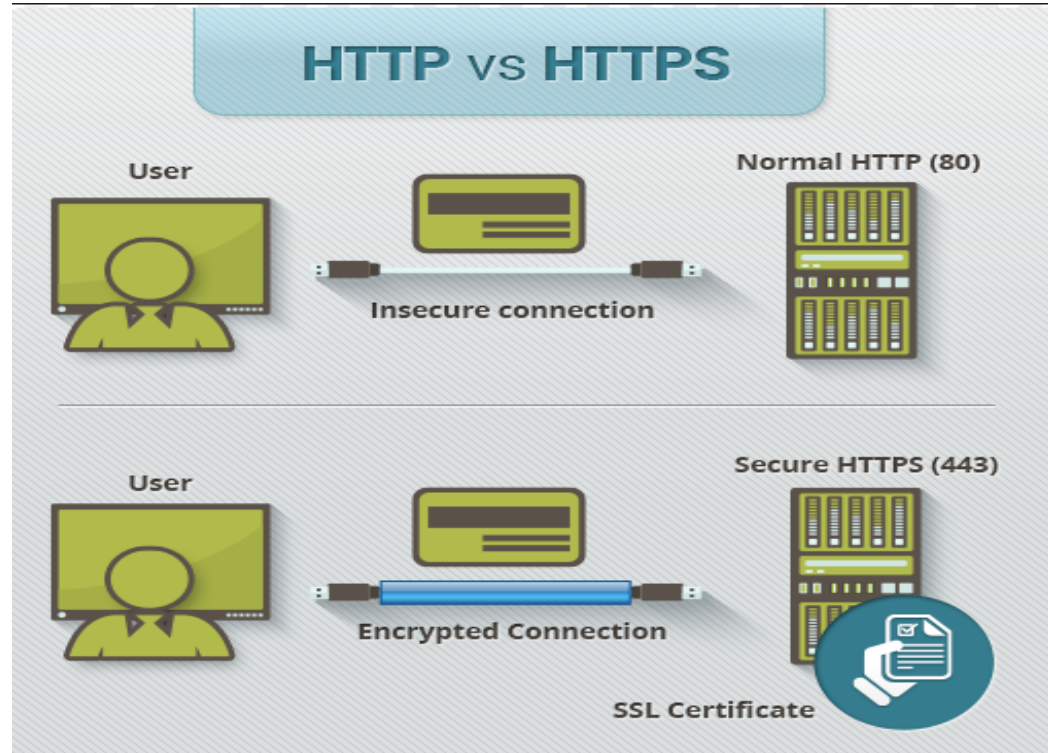
- Input fields for "User ID" and "Password".
- A dropdown menu currently set to "Cards - My Account".
- A checkbox labeled "Remember Me".
- A prominent blue "Log In" button.

Two black arrows originate from the green padlock icon on the left. One arrow points to the padlock icon in the browser's address bar, and the other points to the "https" text in the address bar. A third arrow points from the large green "https" text at the bottom left to the "https" text in the browser's address bar.

What is “HTTPS”?

Hyper Text Transfer Protocol Secure (HTTPS) is the secure version of HTTP, the protocol over which data is sent between your browser and the website that you are connected to. The 'S' at the end of HTTPS stands for 'Secure'. It means all communications between your browser and the website are encrypted.

Helps to prevent hacker attacks that are based on eavesdropping



Anti-Virus, Anti-Malware, Anti-Ransomware

Each is a different type of attack – some just to cause trouble, some to steal information, some to steal “YOU”. It is important to constantly update the anti-virus, anti-malware and anti-ransomware software on a computer because computers are regularly threatened by new types of attacks. These updates contain the latest files needed to combat new attacks and protect your computer.

Your Safety Net: A Backup

- Remember about buying Car Insurance?
- Doing backups is the same, for that: “Just In Case....”
- If your system is attacked and damaged or locked, having a remote location Backup can help restore your computer. Remote meaning not attached to your computer when it is attacked.

Tellico Village Computer Users Club presentation on Backups: April, 2018

<https://drive.google.com/drive/folders/1Fcl3uRCkoSLANF1tD51bw5S-jlsQFJfw>

Conclusion

YOU need to Help Keep YOU Safe

- Guard your Personal Information
- Strong Passwords - Consider Password Keeper
- Be careful on-line – Be cautious of posting Information on Social Media
- Be careful when info requested – others are trying to get you to give them information
- Follow safe “computer” use methods – up to date software
- **Note: The video and slides from this presentation will be made available on-line on the HOA website Watch and Computer Club websites.**

www.hoatv.org

NEWS TICKER > [January 27, 2019] TDOT Liaison Committee Final Report – 2018 > ANNOUNCEMENTS

SEARCH ...

Be Engaged. Be Informed.
Be Heard.



Your Voice in the Village

MY HOA ▾

CALENDAR

HOA NEWS ▾

SOCIAL ▾

BOARD ▾

VILLAGE INFO ▾

LINKS ▾

PRESIDENT'S CORNER

GENERAL MTGS

HIGHLIGHTS &
HAPPENINGS

OUR MISSION

Deliver value to Tellico Village homeowners by providing a 'voice' for homeowner concerns

and engaging programs, while promoting social fellowship, civic responsibility, and providing a



Spring 2019 Courses

[iPad/iPhone](#). Location: Welcome Center Conference Room

[Online Shopping](#): Location: Welcome Center Conference Room

[Windows 10 Basics](#): Location: Welcome Center Conference Room

Tellico Village 
**COMPUTER
USERS CLUB**