



Safe-ER Internet Usage

Protecting Yourself Online

Presented by:
Tim O'Pry
Chief Security Officer

Questions?
cybersecurity@hensslerfinancial.com

Safe-ER Internet Usage

PROTECTING YOURSELF ONLINE



CYBERSECURITY 102

Overview

- Cybersecurity 101 Recap
- Top Three Things NOT to Do
- Web Browsing
- Email
- Social Media
- Public Wi-Fi
- Travel
- What to Do When You're Hacked
- The Dark Web

CYBERSECURITY 101 RECAP

Top 3.5 Things You Must Do for Personal Cybersecurity

1 Use a Password Manager: LastPass



- Use auto-generated passwords with as many characters as the site allows (more characters = more secure).
- Different password for EVERY website.
- Use a unique userID for every site if possible.
- Enable MFA (multi-factor authentication) for LastPass —actually enable MFA where ever supported.

2 Protect Your Most Important Account: Email



- Your email account is the key to your online assets/identity.
- Use MFA. If your provider does not allow MFA—CHANGE!
- Consider using different email addresses for different sites/purposes.

3 Monitor Your Financial Accounts



- Use Credit Karma to monitor TransUnion and Equifax for FREE—enable alerts.
- Sign up for Experian separately.
- Enable all of the available alerts for your credit cards.
- Consider a credit FREEZE if you are willing to put up with the 'thaw' process.

CYBERSECURITY 101 RECAP

Top 3.5 Things You Must Do for Personal Cybersecurity

1 Use a Password Manager: LastPass



2 Protect Your Most Important Account: Email



3 Monitor Your Financial Accounts



3½ Auto Update All Devices



CYBERSECURITY 102

REMEMBER: Security is Inconvenient, but the Alternative is Much Worse.



CYBERSECURITY 102

Top 3 Things to Avoid (or at least limit)

1 Clicking Links in Emails and Downloaded Files



- This is the NUMBER ONE way crooks get to you.
- Remember, links are a convenience—not a necessity.

2 Downloading or Opening Files from the Internet



- If you must, scan the files with your security software first.
- Check links with VirusTotal or BrightCloud.

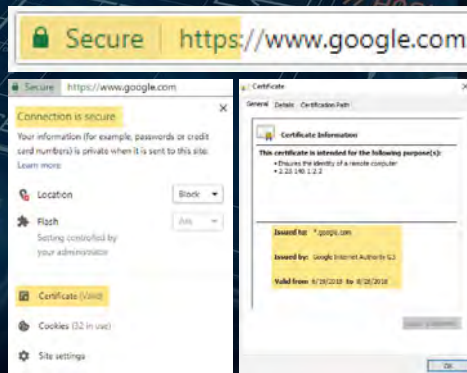
3 Using Public Wi-Fi



- If you must, then limit your activities or use a virtual private network.

CYBERSECURITY 102

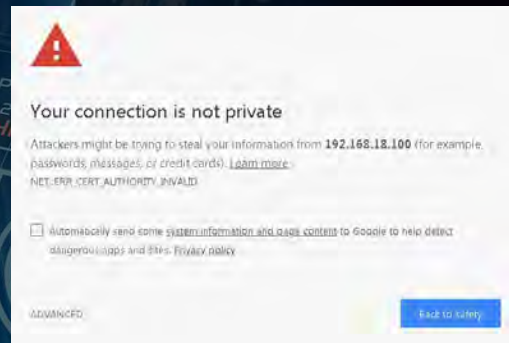
Safe-ER Web Browsing



- Even legitimate, high-profile websites get exploited via ad scamming—don't let your guard down.
- Be very selective in your "clickage."
- Make sure your security software is up-to-date and includes a site checker. We recommend Webroot.
- CLOSE your browser after ending sensitive/banking sessions.
- Be suspicious of any site that is not httpS, and verify each site is what it claims via the certificate.

CYBERSECURITY 102

Safe-ER Web Browsing



- If a website has a certificate that does not match the domain or is invalid, you may see something like this:
- We recommend that you do NOT visit the website.

CYBERSECURITY 102

Trust No One (on the Internet)

- The truth may be out there—but so is your personal information...
- Spoofing is one of the oldest and easiest scams. Learn to look past the name it claims to be “From.”
- After Equifax, Cambridge Analytica (Facebook) and other security breaches of government and private data, we should all assume our basic information is available on the Internet. Once it is, there is no way to “get it back.” So, we must take responsibility for monitoring our accounts.

CYBERSECURITY 102

Phishing, Smishing and Vishing—Oh My!



Phishing is the use of fraudulent emails to induce you to reveal personal information and/or click on links that install malware. This is the primary way crooks exploit the average user.



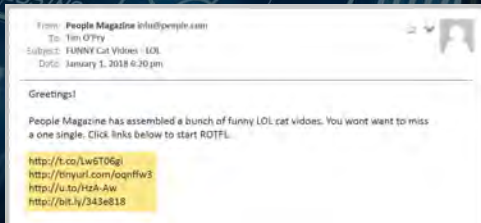
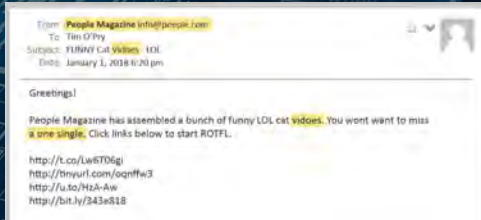
Smishing is the text message version of phishing.



Vishing (voice) are robocalls and spam phone calls that purport to be from the IRS, your bank, the FBI—you name it. They try to scare you into giving them money and revealing personal information.

CYBERSECURITY 102

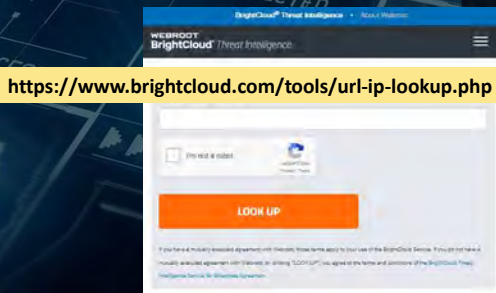
Spotting Fake Emails



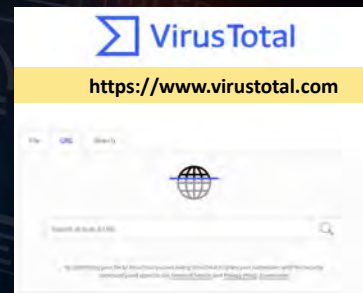
- Assume all links are dangerous until proven otherwise.
- A common tactic is to use a legitimate email and then change the links.
- Look for misspellings and other subtle clues.
- Never click on shortened URLs—these are common in text messages and on social media and look like <http://bit.ly/343e818>

CYBERSECURITY 102

Spotting Fake Emails




- For any site that you have a logon, use LastPass to open and logon to the site, or type in the address “manually” versus using links in emails.
- Use a third party site like BrightCloud or Virus Total to check links and files.



CYBERSECURITY 102

Examining Links



- The text you can see is NOT necessarily the actual LINK (website).
- The text in a hyperlink typically is a different color to make it stand out.
- Hover your mouse over the link BEFORE clicking it to view the actual link (URL). The mouse cursor should change to a hand.
- You can COPY the link to the clipboard by right clicking on it, and selecting "copy."

CYBERSECURITY 102

Social Media Do's and Don'ts



- Majority of attacks on social media are targeted (spearphishing)—and more successful.
- Look out for:
 - Fake customer support accounts
 - Spambot comments
 - Dangerous direct messages
 - Compromised friend accounts
 - Shortened URLs
 - Phony promotions and contests
 - Surveys that share more than you expected (Cambridge Analytica)
 - Changing permissions or sharing settings

CYBERSECURITY 102

REMEMBER: It's Better to be a Passive Viewer versus an Over-Sharer



CYBERSECURITY 102

How and When to Use Public Wi-Fi



- Just say NO!
- Using public Wi-Fi is the high tech equivalent to having unprotected sex.
- Disable the “auto-connect” (Ask to Join) Wi-Fi option.
- Ideally, NEVER use public Wi-Fi—you have no way to confirm your information is secure.

CYBERSECURITY 102

How and When to Use Public Wi-Fi



- When traveling disable Wi-Fi and Bluetooth. Instead, use your cellular connection (hotspot for other devices).
- If you must use Wi-Fi, use a virtual private network (VPN).
 - We recommend Nord VPN: www.nordvpn.com.
 - Even though VPN may protect your connection to external sites, an exploited Wi-Fi hotspot can still expose your device to malware.

CYBERSECURITY 102

Using the Internet While Traveling

- Domestically—use cellular/hot spot or VPN.
- Even in five-star hotels, shared, public Wi-Fi is easily compromised.
- Internationally—cellular hotspot AND VPN.
- Never check your email or logon to any site from any shared device/kiosk (e.g., hotel business center).

CYBERSECURITY 102

I've Been HACKED! Now What?!?!?



- Identify what has been compromised.
- Make a list and start keeping track of the who/what/when/where/why.
- Keep notes on all calls/emails/contacts.



- If your email account was taken over, use the recovery procedure for the vendor to regain control.



- Check your online financial accounts (bank, credit cards, credit reports, etc.).
- File fraud reports and change passwords for any accounts that are compromised.



- If you have been the victim of fraud/criminal activity, once you have identified what was stolen, file a report with your local police department.
- They can usually do this over the phone.



Not sure what to do?
Contact us—we can help.
CyberSecurity@HensslerFinancial.com

CYBERSECURITY 102

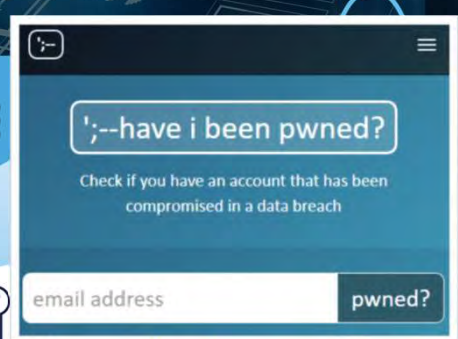
The Dark Web: Why We Need It



- The majority of media coverage is hype, not fact.
- The Dark Web has been used by criminals and terrorists to hide their activities.
- Also used by all major governments, many news organizations, whistle blowers, activists, and people in countries where freedom of the press does not exist.
- Originally created and still funded by the U.S. government, which uses it to provide cover for covert intelligence traffic.

CYBERSECURITY 102

The Dark Web: Fear, Uncertainty, and Doubt (FUD)



Don't Buy It!

- Companies that purport to “let you know if your information is on the Dark Web” are simply using FUD to sell something.
- You can check which of your accounts may have been compromised using: <https://haveibeenpwned.com>

CYBERSECURITY 102

While there is bad stuff and bad people on the Internet, common sense and the basic tactics discussed today will protect you against the vast majority of the common problems.

CYBERSECURITY 102

Recommended Products

Password Manager

 LastPass

VPN for Travel or Remote Access

 NordVPN

Security/Anti-Virus Software

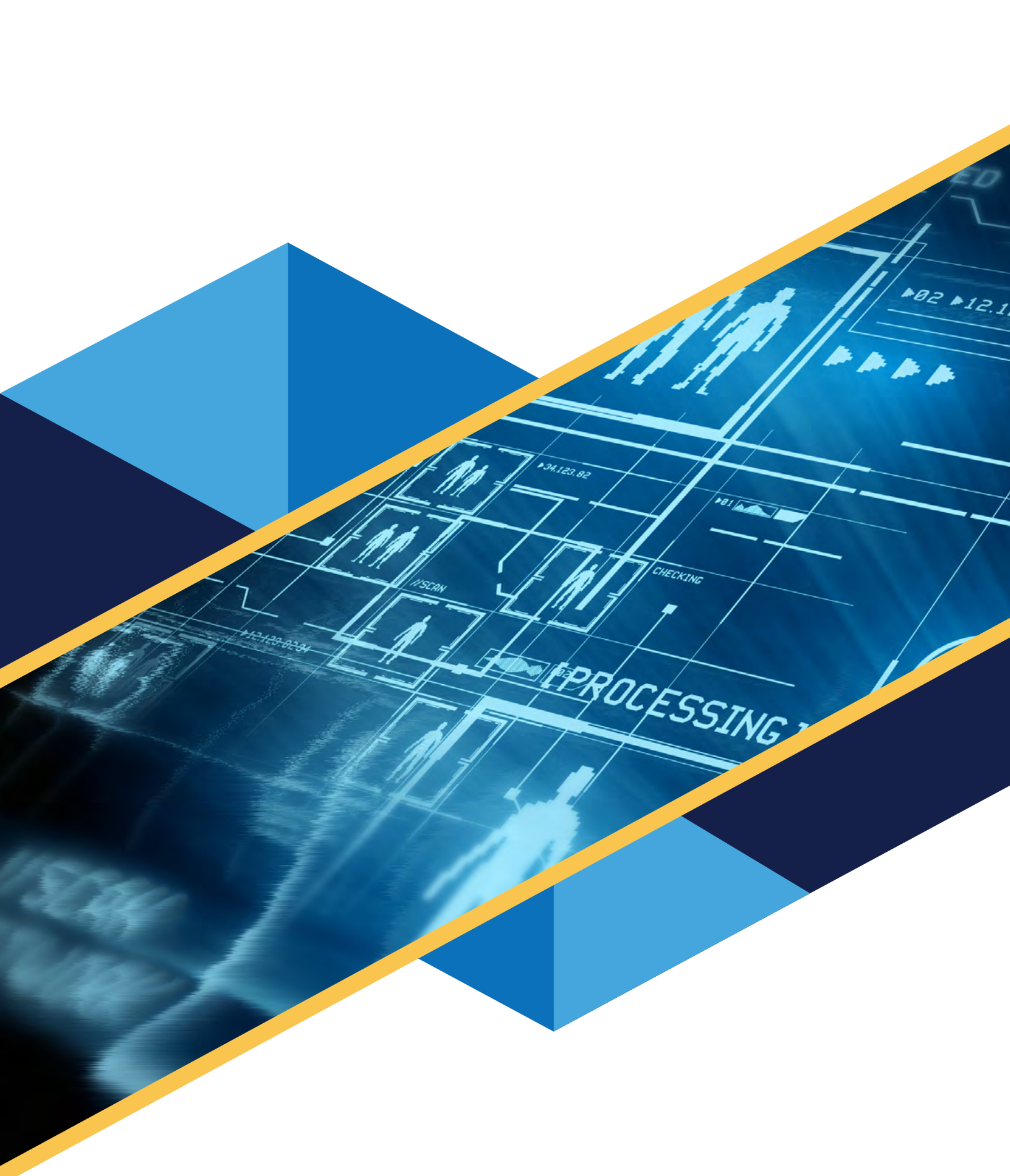
 WEBROOT

Caller ID / Phone Security App

 hiya

Precise and Simple Way to Give Location

 WHAT3WORDS



Henssler Financial shall mean and refer to any and all subsidiaries, parent or sister corporations, limited liability companies, partnerships or other entities or entity controlling, controlled by or under common control with said corporations or entities, including, but not limited to G.W. Henssler & Associates, Ltd., Henssler Asset Management, LLC, both federally registered investment advisers, DiLuzio & Henssler, Inc., Henssler Norton Insurance, LLC, Henssler Insurance, LLC and Henssler Small Business Services, all d/b/a "Henssler Financial." Henssler Financial is not a financial adviser.