

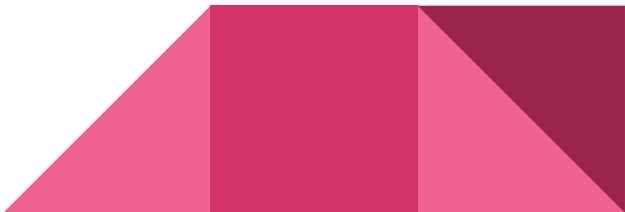
# Keeping Hackers/Scammers Away from your Data and Money

Doug Brent

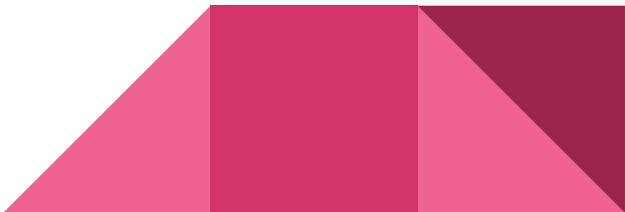
17 November 2020

[doug\\_public@brents.com](mailto:doug_public@brents.com)

# Introduction

- We're going to try some zoom polling to see what other Rotarians have thought and experienced regarding hacking and scamming. All poll responses are anonymous, so no need to hold back.
  - Impact of hacking and scamming is huge, and we all need to take active steps to protect ourselves.
  - I'm willing to bet everyone on this call has made some missteps regarding keeping our information and money secure. Don't be shy or guilty - do better!
  - We'll cover the basic types of cybercrime and fraud
  - Arm you with seven steps to safer computing
- 

# How does hacking/scamming impact you?

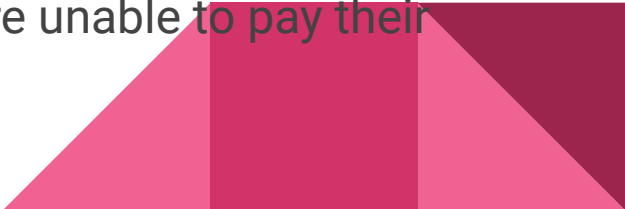
- A 2018 study from the Center for Strategic and International Studies estimated the global cost of cybercrime at \$600B.
  - California is one of the top three states for identity theft (according to the FTC)
  - One estimate (Crowe auditors) of global loss to fraud is \$5 trillion per year
  - 40% of millennials experienced cybercrime in the last year; older people fared a bit better, but lost more money on average
  - Identity theft and computer malware are difficult, time consuming, and may be costly to undo
- 

# Definition of terms


- **Hacking:** using computer technology or social methods of accessing your data, or introducing malware onto your computer
  - Malware: Log every keystroke, make your computer part of a botnet, ransomware
- **Scamming:** Using false information to obtain important personal information or money from you. This could be via a phone call, email, text or mail.
- **Phishing:** (A form of a scam) Using email to get personal information or infect your computer with Malware, usually with a very official looking email or with a link to what looks like a very official (but fake) website



# Hacking example: Ransomware

- You receive an email with a malicious attachment. You open the attachment and the ransomware infects your computer.
  - The ransomware encrypts some or all of the files on your computer and you can't tell anything is happening until a ransom message comes up on your computer. Even if you can remove the malware, your files will remain encrypted, and can only be accessed via a key that the attacker will sell to you (at least about 50% of the time).
  - A 2018 ransomware attack on the city of Atlanta, Georgia left 8,000 city employees without their computers, and citizens were unable to pay their parking bills, water bills and parking tickets.
- 

# Scamming Example: Selling my scooter

- “I'd like to buy it.. I am willing to pick it up tomorrow morning. And I am willing to pay in cash. Or venmo is slightly better if you have it. Does 10am tomorrow work for you? If it does you can send me a text message at my email. Thanks”
  - “We are ready to make the purchase now but we won't be able to meet with you due to our work frame and we are in the process of moving and also preparing for our daughter's wedding, I will proceed to overnight an Official Check to you through USPS tomorrow morning and we will arrange to pick up from you after the check has fully cleared your bank. However, I will be adding extra \$30 to the asking price so that you reserve it for me...”
- 

# Phishing Example

Subject: Your iTunes access has been disabled

From: "App.Support" <no\_reply@appsupport.com>

Date: 2/21/2016 4:33 PM

To: <address removed>@berkeley.edu

Dear User

Your Itunes-ID has been disabled .

You've place your account under the risk of termination by not keeping the correct informations .

Please verify your account as soon as possible.

Ready to check ?

[Click here](#) to get back your account.

Sincerely,

Inc.Apple




You can't stop a  
determined hacker,  
but...





# 7 Steps to Better security


# Step 1: Use multi-factor authentication (MFA)

- MFA means that you use multiple items of information to access a service.
  - For consumers, MFA typically means a password plus the use of a one-time passcode sent via text on a mobile phone.
  - Every major email system, financial institution website, and many others offer MFA.
  - This means that even if someone knows your password, they will not be able to log in to your account without also having your phone.
  - Security experts talk about MFA as “What you have and what you know”
- 

## Step 2: Good and Unique Passwords

- A good password is long, but easily typed without typos; think “pass phrase”
  - Bad: Rotary1
  - Good: FireplaceWindowChairDog@1
- It is essential that each web site and service you access have a different password
  - Hackers take data breaches that include usernames and passwords and immediately test those credentials against every important financial site
- All of this is greatly facilitated with password management software (1Password and LastPass are quite popular); a list that you keep hidden at home is less good, but better than using a common password
- Always change the default password on devices you install at home
  - Wi-Fi router, smart thermostat, security cameras, etc.

## Step 3: Lock your credit file


- The primary reason a thief wants to fraudulently use your identity is to apply for and obtain money/goods with that credit
  - While it is unlikely you'll face a financial loss because of this, it can be very difficult to unwind, and it could negatively affect your credit score
  - Equifax, Transunion and Experian allow you to lock your credit report so that no new credit can be issued in your name
    - And, freezing is now free, and a temporary "unfreeze" is pretty easy
    - See: <https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs>
  - Ideally, you should freeze all three of the credit reporting services, but even one is helpful
- 

## Step 4: Avoid clicking on links in an email

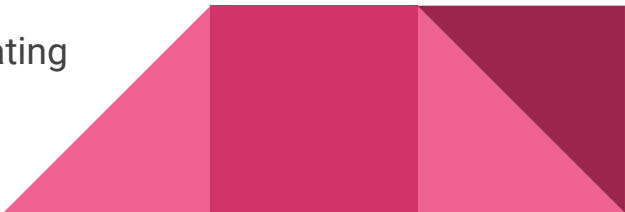
- Phishing emails, and the web sites they take you to are sometimes quite professionally done, and very realistic looking.
- Don't click on a link in an email unless it was something you were expecting to get from someone you know...
  - ...but even that can be a risk, because your friends email might be infected with malware
- If you get a message to update information or retrieve a message from a website, don't click the link, just surf directly to the website, log in, and check for updates there.



## Step 5: Never give out personal information

- No legitimate organization will ask for a password over the phone, email or text - there is never a reason to provide this.
  - Never read back an MFA pass code you receive on your phone to someone else.
  - Unfortunately, your Social Security Number, the source of many tax filing scams, is used fairly widely, but do your best to limit where you provide it.
    - In many cases, when a form asks for your social security number, if you just leave it blank, people don't push the issue
  - Take care with social media postings, photo postings (every photo has a location in it by default), vacation responses, etc.
- 

## Step 6: Move to a more simple/secure device

- Windows computers are ubiquitous, powerful, general purpose computers that have about a 90% market share
  - Because Windows is everywhere, hackers first target Windows computers - it is simple economics and has been for decades
  - For people who are IT-savvy, Windows is a great choice
  - For everyone else, an iPad or Android tablet is much easier to keep up and operating, and is more secure against malware
    - These are not general purpose computers, and it is easier to maintain a secure application ecosystem.
    - And, even these devices have security flaws; enable auto-updating
- 

# Step 7: Use common sense and the right tools

- If it sounds too good to be true...
  - You didn't win a vacation, a timeshare, or a new car
  - If the IRS or Social Security or Apple Support want to find you, they won't call your phone.
- SMS/text scams are growing in popularity, and someone may even use your name. If you don't recognize the phone number, don't respond.
- Payment platforms like Apple pay and Google pay are more secure than a credit card, because the merchant never sees your credit card number.
- Credit cards offer you more loss protection than debit cards; stick to credit whenever possible





# Do You Choose Security or Convenience?

1. Multi-factor authentication on every important account (MFA/2FA)
2. Good and unique passwords, ideally using a password manager
3. Lock your credit file
4. Avoid clicking on a link in an email
5. Never give out a username or password in an email or over the phone
6. Move to a simpler, more secure computing device
7. Use common sense and the right tools





Q&A