



# Internet Safety



SM Roger Aylstock  
April 21, 2020





# Agenda

- Common scams and how to watch for them
  - Social Media
  - Email
  - Phone
- Password Managers





# Common Facebook Scams

- **Social Media Quizzes**

- Quiz: What Dr. Seuss Character Are You?
  - Q: What was your high school mascot?
  - Q: What was your first car?
  - Q: What was the name of your first girlfriend?
  - Q: What is your favorite pet?
  - Random generator: "Cat in the Hat"
- These are common security questions asked by banks and credit card companies.
- Be careful. Free quizzes offered on social media actually aren't free — you're paying with your personal data that big data companies collect for targeted advertising, or cybercriminals collect to sell on the dark web.



# Common Facebook Scams, cont.

- Fake Links/Click Jacking – Fake news, free giveaways, etc. can be delivery methods for malware. Just like email scams of the past, these leverage stories, news or offers that catch your attention. The point is to have you click on a link or share something that propagates malware. Examples include:
  - Direct Messages with links or attempts to get you to look at something.
  - Links resulting in another login request for Facebook/Email Provider – this is to harvest your account.
  - Seeing a friend request from someone that is already your friend.
  - “Grandpa, I’m in jail in a foreign country, can you send money? Don’t tell my parents!” has migrated to Facebook with a different twist.



# Common Facebook Scams, cont.

- Free Taco Bell tacos (or McDonalds hamburgers or Chick-Fi-a sandwiches), twice a week for a month. Like and share and we'll send you a coupon (or fake coupon image included).
- The big prize giveaway. Most common recent bait includes a Disney-related prize and an SUV or luxury vehicle. Some current scam pages have upwards of 60,000 "fans." URL [www.disneygiveaway345.com](http://www.disneygiveaway345.com) Looks legit, right?





# Common Facebook Scams, cont.

- **“SEE WHO’S VIEWED YOUR PROFILE!”**
  - This scam is a form of “clickjacking”, luring you into clicking on a link by promising some sort of desirable incentive, and instead leading to an online survey that will earn a commission for the scammer. Sometimes, the survey will even collect personal information about you, with which the scammer can then use or sell as they see fit. Keep in mind that Facebook does not track this type of information, nor would they share it with the public if they did.
- **FACEBOOK “DISLIKE” BUTTON**
  - This scam urges Facebook users to enable a “dislike” button on their account to allow the added capability of “disliking” a post. However, when you click on the ad to “enable” the button, you will either be taken to a survey scam or inadvertently install malware on your device.





# Most Common Social Media Scams

- **FREE GIFT CARDS** (COMMONLY FOR STARBUCKS, CHEESECAKE FACTORY, OR VICTORIA'S SECRET)
  - Offering a "free gift card", often in return for sharing the original post, this phishing scam attempts to get you to divulge personal information and may also sign you up for services you neither want or need.
- **FAKE CELEBRITY NEWS**
  - For example, "Justin Bieber's been stabbed!", generally accompanied by an image or photo that seemingly verifies the claim. False celebrity news reports are a relatively assured way to get clicks, but are also a guaranteed method to risk a phishing attempt or get a malware download onto your device.
- **"YOUR ACCOUNT HAS BEEN CANCELLED."**
  - This phishing attempt, seemingly from your social media provider, informs you that your account has been cancelled in order to lure you into providing the scammer with your username and password, which they can then use to access the more detailed information about you located on your social media profile. Remember, if you ever need to verify anything about your account, go directly to your social media site. Never trust the link provided in the message.



# What online behaviors should I watch out for?





- To protect yourself from scammers, watch out for the following:
  - People asking you for money who you don't know in person.
  - People asking you for advance fees in order to receive a loan, prize or other winnings.
  - People asking you to pay for something through weird products such as Apple Store cards, Western Union, store gift cards, etc.
  - People asking you to move your conversation off of Facebook (example: a separate email).
  - People claiming to be a friend or relative in an emergency.
  - Poor spelling and grammar mistakes.
  - Pages representing large companies, organizations or public figures that are not verified.





# Email Scams

- “CONFIRM YOUR ACCOUNT”
  - Similar to the previous entry, this is a phishing attempt designed to trick users into providing private information, specifically their email address and password.

▲ From: American Express: 5 item(s), 5 unread		
 American Express	[SPAM] Your bill payment could not be completed	Sun 4/19/2020 12:44 PM
American Express	[SPAM] New Important Online Message	Mon 4/13/2020 4:43 AM
 American Express	[SPAM] Confirm your account mobile number	Fri 4/10/2020 10:41 PM
 American Express	[SPAM] Verify your contact number immediately	Fri 4/10/2020 9:58 PM
 American Express	[SPAM] Please confirm your account contact details	Fri 4/3/2020 5:38 AM
▲ From: aylstock.com: 5 item(s), 5 unread		
aylstock.com	Deativation	Tue 4/14/2020 1:28 AM
aylstock.com	[SPAM] DeActivation	Mon 4/13/2020 8:24 PM
aylstock.com	[SPAM] DeActivation	Mon 4/13/2020 7:24 AM
aylstock.com	[SPAM] Quota Limit Report	Thu 4/9/2020 6:38 AM
aylstock.com	[SPAM] ACCOUNT SHUTDOWN NOTIFICATION!!	Fri 4/3/2020 10:05 AM



# Email Scams - How to keep from being scammed

- Don't click links or open files in emails if you are not sure who they are from.
- The "FROM:" address can easily be faked.
- Don't pay through Apple Store cards, Western Union, store gift cards, etc.
- Be skeptical about free trial offers.
- Don't deposit a check and wire money back.
- Talk to someone. Before you give up your money or personal information, talk to someone you trust.



# Common Phone Scams

- **Threatening Calls From the IRS**

- Especially popular during tax season, IRS phone scams involve crooks impersonating federal agents. They sound official and may even provide a badge number. If immediate payment isn't made, they threaten lawsuits or may say the police are on the way to make an arrest.

- **Technical Support Calls**

- In this scam, the caller typically says they are from a well-known company like Microsoft or Apple and have detected an error on a person's computer. They will then talk the victim through a series of steps to "fix" the problem. In reality, a person is unwittingly downloading software that will hijack their system or give the caller remote access.





# Common Phone Scams - How to keep from being scammed

- Don't answer your number if it is from a number not in your address book. Most legitimate callers know how a voice message works and will leave one. (Sometime scammers will too but not usually)
  - Google the number to see if it is a legit business or if there have been scam/telemarketer reports.
- If you happen to answer the phone and realize this might be a scammer, just hang up. Don't give out any personal information. You can easily block the number if they continue to call.
- If you are not sure if it is really say your bank, get their name, hang up and look the bank's number on the internet then call that number.





# Install Your Phone Carrier's Spam App

- AT&T has an app on the App Store called CallProtect. Other carriers may have a similar app. This app detects and blocks calls from fraudsters and helps identify telemarketers and other suspected spam calls. When a call comes in, AT&T looks the number up in their database and it pops a message on my phone like "Telemarketer." No, thanks; I'll not be answering that one today.





# Let's Talk Passwords

- Don't use the same password on all the sites you visit. Here's why:

**2019 DATA BREACHES**

- JANUARY MARRIOTT HACK, 383 MILLION CUSTOMERS
- APRIL FACEBOOK ERROR, 540 MILLION RECORDS
- SEPTEMBER WORDS WITH FRIENDS HACK, 218 MILLION ACCOUNTS

**SOURCE:** CNET, 2019 Data Breach Hall of Shame

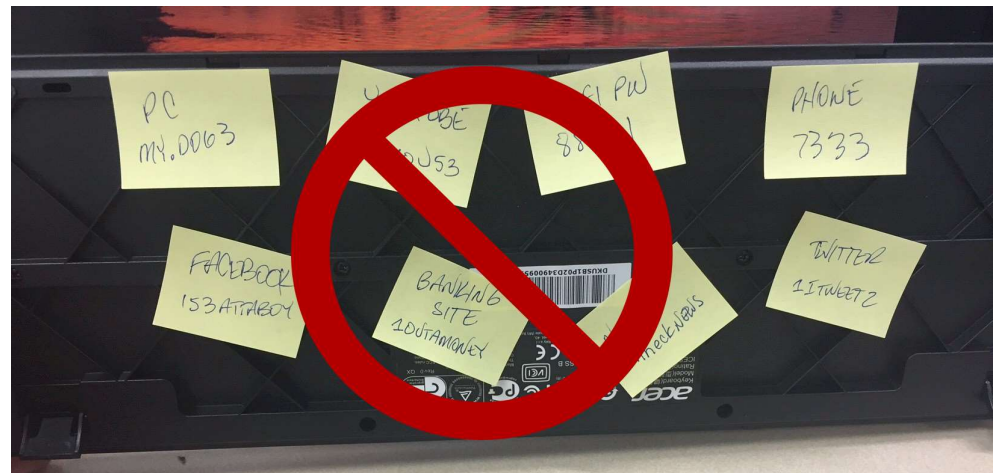
The infographic is set against a blue background with a faint American flag pattern and silhouettes of people. The text is in white, with the title in a large, bold, sans-serif font. The list items are in a smaller, bold, sans-serif font. The source is at the bottom in a smaller, bold, sans-serif font.





# Get and use a Password Manager

- Your keyboard look like this?
- Get a Password Manager to manage your passwords (and much more)
- A Password Manager can securely store your user information





# Password Manager

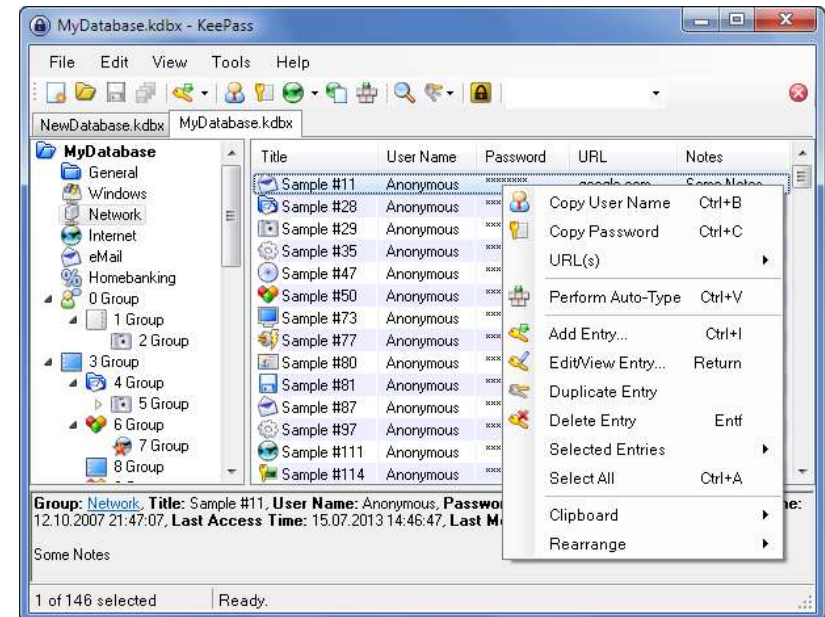
- Realize that a password manager can store much more than just access passwords. In my personal password tool, I have a section for:
  - Autos where I store VIN numbers, License Plate Numbers and expiration dates.
  - Banking section has my back account and routing numbers, PINs, bank phone numbers and username/passwords.
  - Credit Cards section has all my credit card numbers expiration dates, security numbers, and bank phone numbers. If my wallet was ever stolen, I have easy access to all the numbers to report cards stolen. I wouldn't have to sit around and try to remember "What's in your wallet?"
  - Insurance section has my policy numbers for the house and auto, the agent name and contact info.
  - Medical section has prescription numbers, doctor and pharmacy names and addresses.
  - People section that has all my spouse, kids and grandkids birthdates and anniversary dates.
  - Travel section has all my frequent flyer numbers and car rental companies.
  - Web Logons section has the username, password and URL for all my web logons. Including security questions and answers.
  - My password manager not only manages my passwords, it helps manage my LIFE!





# Some Password Managers

- **KeePass (desktop)**  
(<https://keepass.info>)
- KeePass is a free, open source, lightweight and easy-to-use password manager. You can put all your passwords in one database, which is locked with one master password. The database are encrypted using the best and most secure encryption algorithms currently known.





# More Password Managers

- **Dashlane** <https://www.dashlane.com/>
  - Dashlane is another free password manager. They also have a paid version (\$4.99/mo) that allows backup to the cloud and device sync across other devices such as your phone.
- **LastPass** <https://www.lastpass.com>
  - LastPass is a cloud-based, subscription password manager. They have a Family plan for \$4/month.
- **eWallet** <http://www.iliumsoft.com/ewallet>
  - eWallet is a digital wallet that is my personal favorite. It is available for Windows PC, iPhone, iPad, macOS, and Android. It is a paid product with one-time cost of \$9.99 to \$19.99 depending on device. You can easily synchronize data from say a PC version to your iPhone with just a few clicks.



# Questions?

