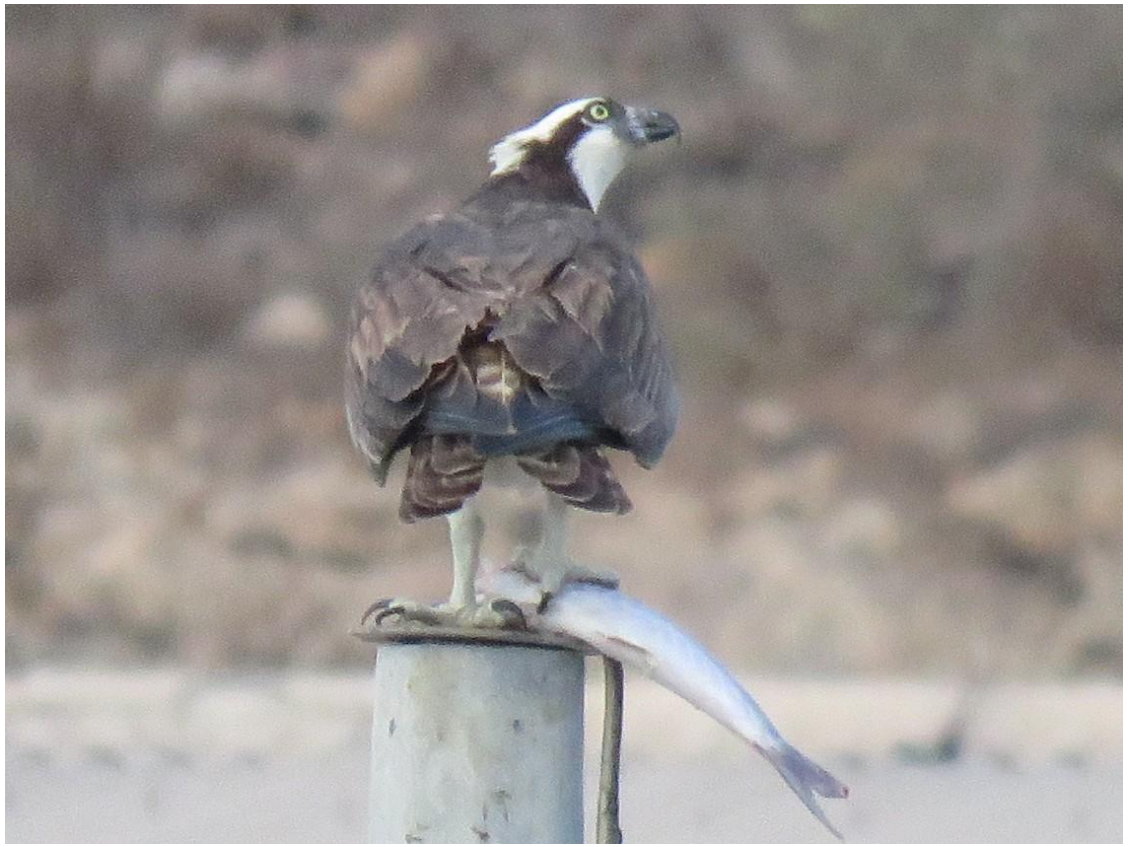
The Future Of Protection



Ray Carlson

Prescott Computer Society

General Meeting

December 2018

The Need for Protection – Recent Example

Marriott/ Starwood Data

- **A huge database was hacked** including names, addresses, phone numbers, birthdates, travel dates, passport numbers, email addresses, passwords & credit card numbers.
- The **immediate risk is credit card numbers** with expiration dates & codes – encrypted but the data to descramble was included.
- Credit card company should cancel charges if notified in reasonable time & should issue new ones so risk is limited.
- Passwords are a risk if used with same username on other sites.
- Passport no. can be used to submit change of address if thief is good at generating fake passports – but that is difficult.
- Knowledge of upcoming travel can be used by burglars.

The Future Of Protection – Recent Example

- Another **major risk is for the crooks to open new accounts** in your name so monitor or freeze credit.
- For some, there may be risks from **documenting their schedule including bribes.**
- Encouraging is the fact that sales of this data have **not been identified on the Dark Web.**
- Such listings usually appear quickly so purchaser can use the data before canceled or changed.
- May be intended for mail &/or phone **marketing or phishing**.
- An internal security tool indicated a possible breach in **September**, but the it took until **mid-November to** decrypt the database sufficiently to clarify what had happened..

Recent Examples of Data Breaches

- A security warning tool spotted the loss on September 8, 4 years later, and, due to complexity, security consultants took until November 30th to determine what was happening.
- Marriott announced **an "unauthorized party had copied and encrypted information, and took steps towards removing it."**
- Up to **500 million** records were copied but 173 million only included names & addresses &/or email addresses.

Recent Examples of Data Breaches

- The loss only affected Starwood hotels including: **W Hotels, St. Regis, Sheraton Hotels & Resorts, Westin Hotels & Resorts, Element Hotels, Aloft Hotels, The Luxury Collection, Tribute Portfolio, Le Méridien Hotels & Resorts, Four Points by Sheraton and Design Hotels** in several countries.
- The access **started in 2014,** 2 years before the merger with Marriott. The two chains have not yet merged their data bases.

Recent Examples of Data Breaches

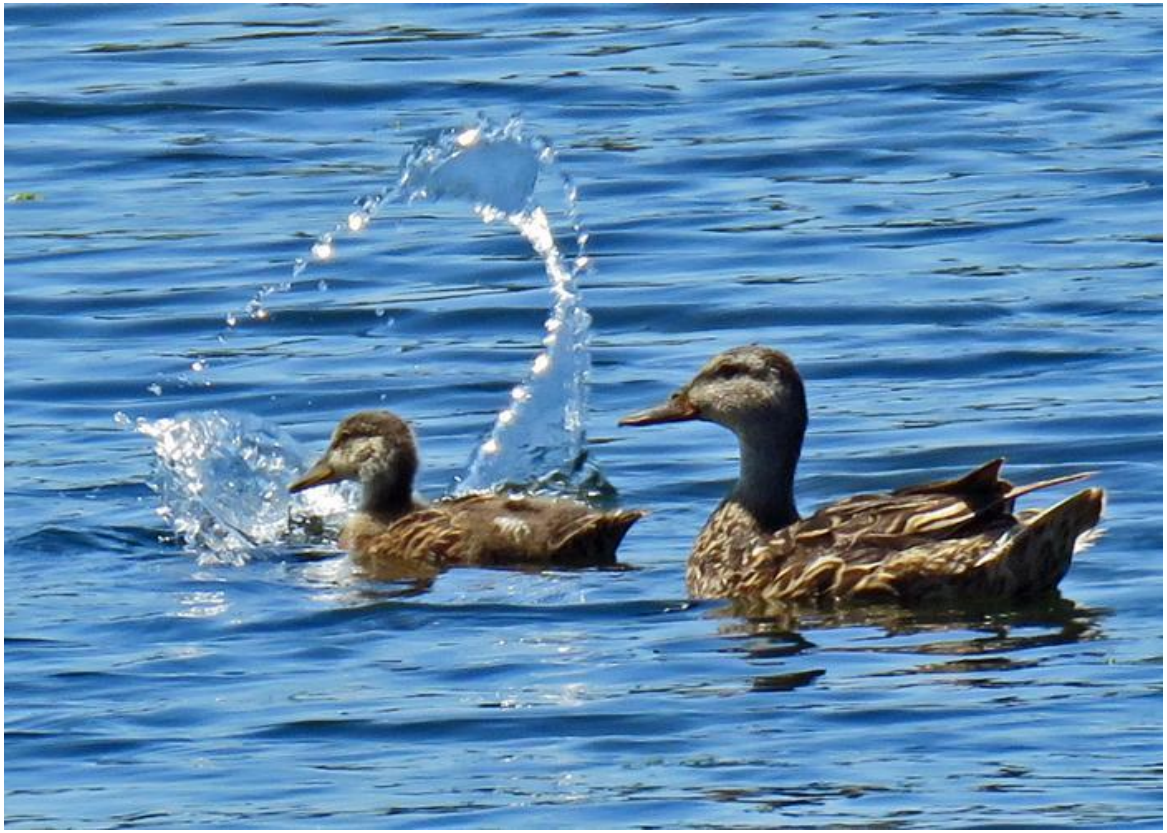
- Usually when financial data is hacked, it quickly shows up for sale on **the Dark Web** before credit card data can be changed.
- In this case, no such sale has been recognized suggesting the thief's goal may not be the credit card information.
- The data can be used to **generate fake identities, for marketing, for blackmail** through compromising data, etc.
- Sheraton had a previous problem in 2016 with malware in its restaurant/ gift shop system taking payment details – there is a tendency for companies that have one loss to have more.
- Marriott has cyber insurance to help with resultant losses for the company, but the coverage is complicated &, for the customer will only cover what Marriott is allowed to reimburse.
- Marriott has security consultants trying to determine what happened.

Other Recent Examples

- **Quora,** the online question & answer service, was breached resulting in the names, email addresses, encrypted passwords, settings and IP addresses of **100 million customers** to be viewed. Users provide personal description & credentials.
- The attack was "by **a third party who gained unauthorised access** to one of our systems" including personal information.
- At the **Cancer Treatment Center in Phoenix** on September 26, officials discovered an email account was hacked, after an employee fell victim to a phishing attack on May 2. The employee shared the network log-in credentials in response to a fraudulent email that appeared to be sent from a CTCA executive.
- The log-in was changed a few hours later but allowed time for a hacker to have access for a few hours to patient information.
- This was at least **the 10th healthcare phishing attack in the 3rd quarter of 2018**

Responses to Such Examples

- **Google** has a high risk of such breaches due to having 85,000 employees with access to its data base. It **successfully protected** itself by mandating use of security keys.
- The US Congress has **proposed legislation** to force companies & administrators to face fines and jail time for **allowing** such breeches. Such laws were passed in Europe. This event might generate support for passing those bills. But there is pressure to avoid regulations.
- Attorney Generals in New York, Massachusetts, Maryland and Illinois have opened investigations into the appropriateness & timeliness of Marriott's actions, but, unlike Europe, the US has limited laws penalizing companies that experience losses.



What Can the User Do?

Approximately **3.3 billion credentials** were stolen in 2017 with **81 % of the breaches apparently due to weak/stolen passwords**

To Offset these problems --

- **Monitor credit cards & credit reports, e.g., Credit Karma, for signs of fraud;**
- **Change passwods as frequently as possible through a password manager - LastPass or Dashlane - or through a security key;**
- **Encourage pressure on companies that have data bases of user names, passwords, credit card details , and the like to have effective control; of that database.**
- **Googles use of security keys offers an example.**

The Future Of Protection

- **Anti-virus programs** are useful for monitoring attachments, new software, apps & websites.
- **Passwords** have been viewed as the key to identifying the user to the computer and sites on the Internet.
- Currently, the assessment of passwords has changed defining them as a **particularly weak facet of protection** because:
  - A good hacking program can guess some passwords because of recognizable words or use brute force attacks if the password has a smaller numbers of characters.
  - Hackers can look for a repeat of previously hacked words.
  - And so on.
- The **biggest risk,** though, is sloppy company procedures that regularly allow theft of clients' passwords.
- A consortium of major Internet companies have proposed procedures to **replace passwords** with safer protections.

2-Factor Authentication

- A key to improving protection is to **have 2 reliable types** of protection so one can offset any weakness in the other..
- **Biometrics** such as fingerprint readers, facial or iris recognition, or the like can help but vary in quality & ease of access.
- **Texting** or emailing a code is good but can be intercepted or ineffective if phone/Internet access is lost.
- **Behavioral** biometrics consider a large number of behaviors such as pressure on keys, speed of typing, hesitations, use of key combinations, etc. It looks for those for an individual that most differ from the average user & puts together a distinct profil. Early tests are encouraging but need to be expanded.
- A new alternative with encouraging results is the use of **security keys** that generate unique codes identifying to the software or website the user involved.

Security Keys

- What makes security keys better?
  - Security keys send **a unique code that changes** each time it is used
  - Passwords stored in a **password manager** can be changed with every use but depend on remembering a master password & don't help with initial sign-in;
  - **Codes sent by text** can be intercepted;
- Some auto keys send radio signals to the car to unlock it, but clever criminals have used a set of signal relays to unlock the car when the key is in a home or office;
- Codes sent by **apps like Duo Mobile or Twilio Authy and Google Authenticator** are safe for a phone;
- Microsoft has just announced connecting security keys to the **Hello page** that opens Windows 10 - currently needs an app

Evolution of Security Keys

- In **2011**, **Yubico** invented the concept of a single security key to protect user accounts from phishing and unauthorized access. They **worked with Google** to further develop this concept creating the FIDO U2F standard.
- Now, Yubico has worked in collaboration with Microsoft & others to create **FIDO2.** With FIDO2, the Security Key with its strong authentication can now handle different tasks:

— **second factor** in a two factor authentication solution - for Google, Twitter, & Facebook

— **strong first factor,** with the possession of the device only, allowing for a passwordless experience- just tap and go

— **multi-factor** with PIN to unlock device & tapping key to authenticate is recommended such as financial transactions, or submitting a prescription.

- Having 2 keys is now recommended in case 1 is lost or stolen.

Security Keys

- A usb-based key can **create a security code** and transmit it to the computer, browser, and key websites.
- According to an evaluation by PC Magazine, **Yubikey 5 i**s
  - The **fifth generation** of this company's keys;
  - Durable & reliable with no moving parts;
  - **NFC (**Near Field Communication) capable so with a phone or tablet can connect by tapping;
  - **Different connectors f**or different types of usb slots;
  - Supports FIDO U2F & FIDO2, the **standards built for sign-ins** that proves your identity;
  - Generates 6 digit one-time user passcodes;
  - Supports multiple protocols for other security roles.
- Negatives:
  - Relatively Expensive.
  - Requires effort and education to fully realize its potential.
  - **Limited iOS integration**.
- See https://www.pcmag.com/review/363889/yubico-yubikey-5-nfc

Use of Security Keys

- Currently **works with** Google, Windows, Twitter, Facebook, Dropbox, Dashlane, LastPass, KeePass, 1Password, PasswordSafe, Linux, GitHub, GitLab, Salesforce, aws,PushCoin, Bitbucket, and others.
- For instructions for each, see: https://www.yubico.com/setup/#yubikey-5-series
- As a **browser, can use Chrome, Firefox, Opera, or Edge BUT.**
- With Google, go to the 2-Step Verification section of your Google Account. Select Get Started and then Next before inserting key.
- Tap or push disc or gold tip or button.
- You will be asked if Google can see the type of key.
- Follow the instructions and add “recovery info & backups” in case the key is lost.
  - Green LEDs to let you know you're connected and functioning.

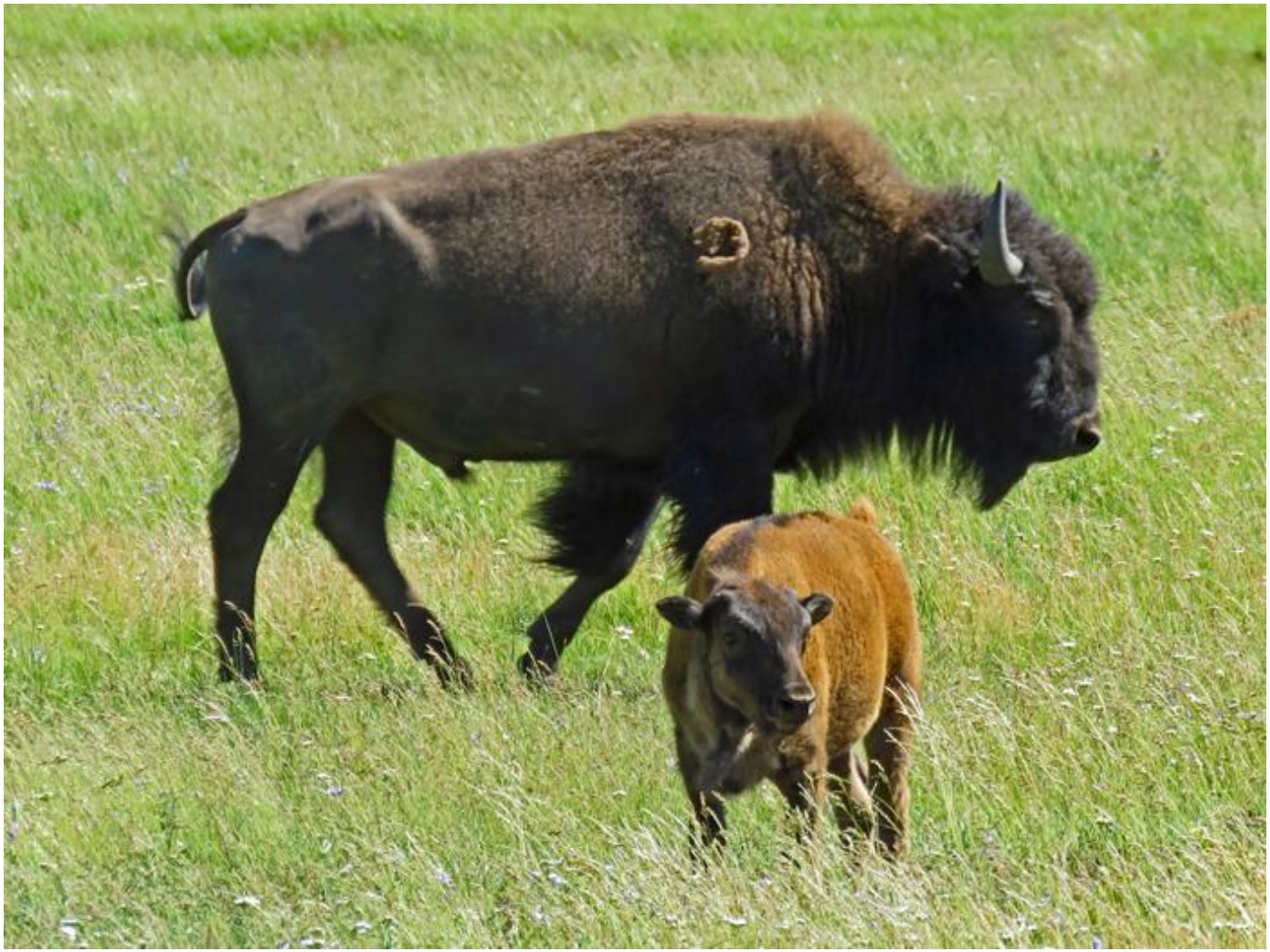
Use of Security Keys

- Add the key to protect the computer --
- Sign in to your Google Account.
- **Since you set up 2 step, it will ask you to insert key.**
- **Tap or push disc or gold tip or button.**
- Select “Don’t Ask Again On This Computer” & add whatever is asked.
- After this, If anyone tries to sign in to your account from another computer, will ask for your security key
- If the key is lost, you will need to use one of the following based on which has been set up:
    - Verification codes, Google prompt, Backup code, or a different security key you’ve added to your account
    - A registered computer where you previously chose not to be asked for a verification code
- Otherwise, you have to contact Google & answer questions & wait

Use of Security Keys

- Insert the YubiKey into the appropriate slot when prompted.
- Just **tap the gold disk** (or metal tabs, depending on the model), and the service enrolls your key.

- 's it!**With phone, can select NFC, tap key on back of phone** until makes a connection and proceed - can take multiple tries;
- **With phone, can select NFC, tap key on back of phone** until makes a connection and proceed - can take multiple tries;



Use of Security Keys

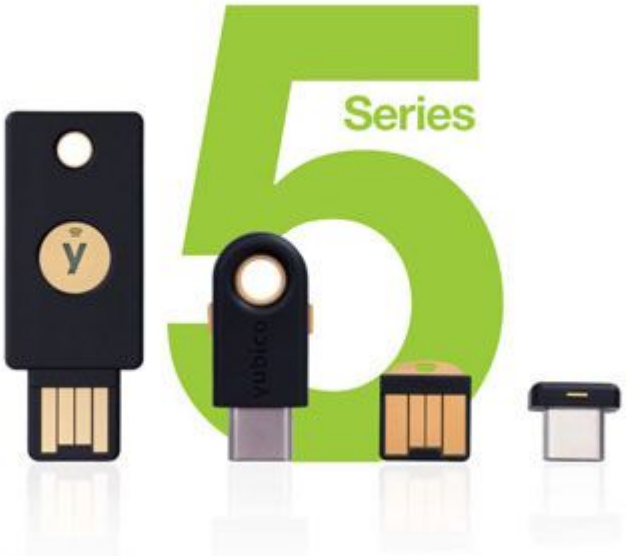
- Google does not encourage use of NFC since signal can be intercepted.
- NFC works with Android but, at this time, **not iOS;**

- With a **password manager** like LastPass or Dashlane, go to Settings & click on text & tap button on key.
- The key will generate unique passwords for each site.
- Next time you connect, it will request the key.
- There is an **Advanced Security Program** for people in high risk professions like journalists or activists.

Use of Security Keys

- With the Windows 10 Anniversary Edition (build 1607), any YubiKey 4 Series, or YubiKey NEO will work with **Windows Hello** for device unlock.
- Download the **YubiKey for Windows Hello app** from the **Microsoft Store**, and follow the instructions in our **Getting Started Guide**.
- With older versions of Windows 7, 8, or 10, insert your YubiKey and log in with your account password.
  - Set up includes **installing a small utility from Yubico to secure access in challenge-response mode.**
  - Once set up, this feature works **without an internet connection.** It does not work with Microsoft Cloud or domain accounts.

Yubico Security Keys



- Yubico offers **a variety of choices:**
  - The Yubikey 5 NFC = $45 which adds a wireless connection to a phone thrtough NFC- Near Field Connection;
  - The Yubikey 5 Nano = $50 which doesn't stick out as far;
  - The Yubikey 5C = $50 which connects to a usb C;
  - The Yubikey 5C Nano = $ 60 which combines the previous 2..
  - For businesses, each one can function as a Smart Card (PIV), can generate one-time passwords, support both OATH-TOTP and OATH-HOTP, and can be used for challenge-response authentication. All four devices support three cryptographic algorithms: RSA 4096, ECC p256, and ECC

Software Alternative to Security Keys

- **The** Google Authenticator **generates 6 digit passcodes every 30 seconds, but Yubico has its own Authenticator app which works easier with the key.**
- **On a new device with that app installed, select option to install new device. A QR code will appear. On the menu, select option to capture QR code.**
- **Tap key on back to generate a code for the phone.**
- **The Google version stores the codes for this program on the computer, but the Yubico version stores them on the key making them unavailable to hackers, etc. - 4.3 ***

Software Alternative to Security Keys

- **There are also Android apps that generates codes for phones. The**
  - **Authy** is one of the more dependable two-factor authentication apps. It works similarly to Google and Microsoft's variants. You get codes from it and use them to authenticate your login. It works pretty well. The app also comes with offline support, device syncing, and it supports most popular websites and account types -- 4.2*
  - **FreeOTP Authenticator** is a free and open source authenticator app. It works with most popular accounts, including Facebook, Google, and many others. You also get support for productivity sites like GitHub. It also boasts support for businesses as long as they support TOTP and HOTP. That makes it a fairly cheap solution for small businesses. It's not the most popular option for authenticator apps, but it works exceptionally well - 4.5 *.

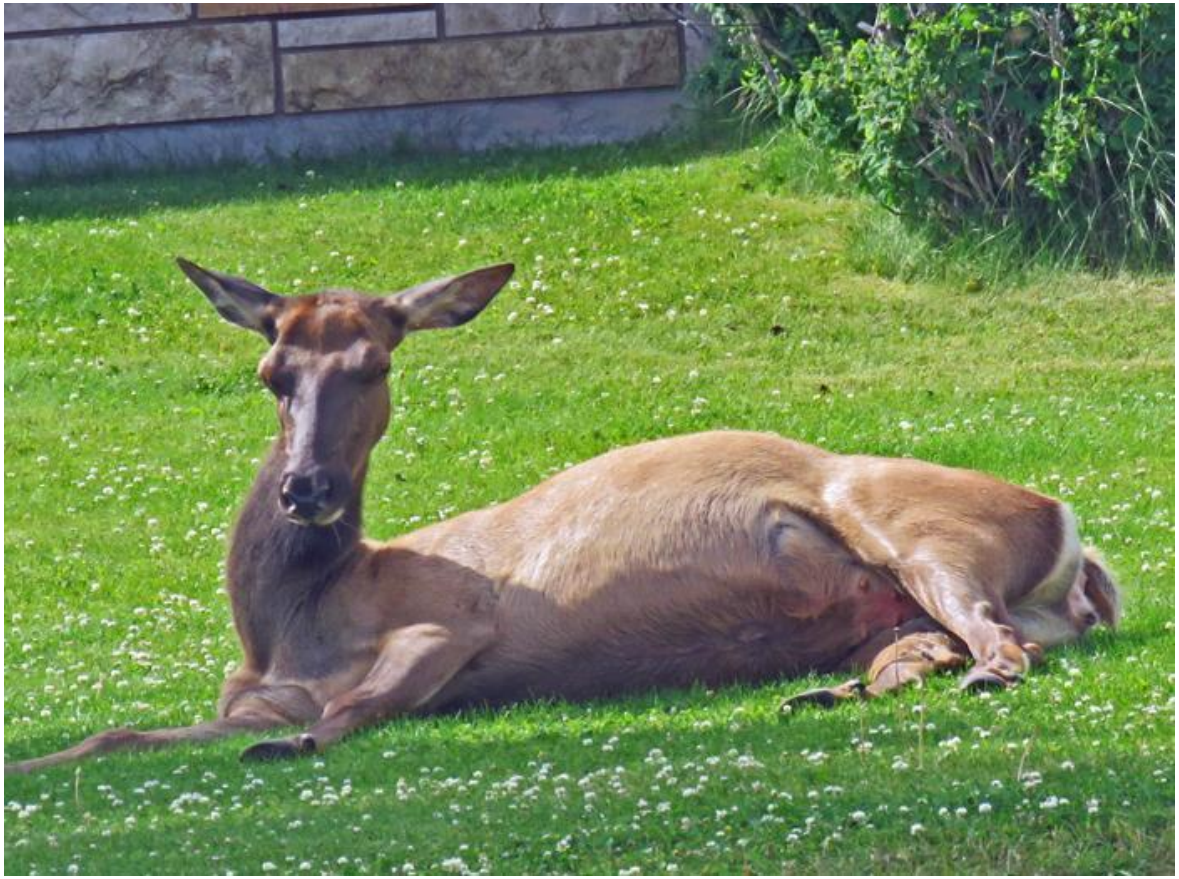
Software Alternative to Security Keys

- **There are also Android apps that generates codes for phones.**
  - **Microsoft Authenticator** is Google Authenticator's biggest competitor. It's popular, it works well, and it works for stuff other than Microsoft apps. Otherwise, it's actually a fairly simple app not unlike Google Authenticator. You log into a site or an app, it asks for a code, and you open this app to get one. We usually recommend Google Authenticator to people who use Google services heavily. The same goes for Microsoft. Those who use Microsoft heavily will likely be more comfortable with this one than most of the other apps on the list. It's also free with no ads or in-app purchases.- 4.1 *.

Titan, Feitian, Thetis Security Keys

- Google developed a competitor called the Titan.
- Android has not been enabled for this key, so its use is with computers only.
- They do not work with TOTPs, Smart Cards, LastPass nor communicate wirelessly.

- This makes it simpler while less competent.
- The cost is 2 for $50 with a USB-C adapter and a Bluetooth micro slit key fob included, half price.
- Other lower cost ones include the Feitian Multipass for $40 & $25 & epass for $18 and Thetis folding design for $20.
- See Amazon for reviews of these alternatives



The Future

- Currently, the keys are used by major browsers, some computer logins & some software.
- The pattern of what works with what is confusing forcing thought about what risks are greater for yourself and those whose information you control.
- Each year should show an increase in what is available until in a few years, the keys will be necessary.