Essential Steps

Reducing Your Personal Attack Surface

Actionable Tactics To Protect Yourself & Family

Plurilock
CRITICAL SERVICES

The following recommendations in this document will help prevent:

- ID Theft & Credit/Loan Fraud
- Banking & Check Fraud
- Tax Filing Fraud
- Personal Account Take Over Attacks
- Impersonation & Social Engineering Attacks
- Extortion Schemes
- Corporate Attack Take Over & Social Engineering Attacks
- Targeted Scams & Online Stalking
- Reducing Scam & Spam Calls/Messages
- Preventing SIM Swapping Attacks
- Preventing Fraudulent Credit/Debit Card Charges

Note: None of the services mentioned in this presentation are sponsored by Plurilock or the author of this guide.
No warranties are provided for any of the services discussed.

Plurilock CRITICAL SERVICES

What is a Digital Footprint?

Definition and Types of Digital Footprints:

A digital footprint is a trail of data you leave behind while using the internet, which can be categorized into active and passive footprints.

- An active digital footprint refers to the intentional data you share online through activities such as social media posts, online shopping, and content creation.
- For example, every tweet you post, product review you write on Amazon, or video you upload to YouTube contributes to your active digital footprint.
- A passive footprint is the data collected without your explicit knowledge, like browsing history, location data and personally identifiable information shared by databrokers. Each action leaves a trace that can be collected and analyzed, sometimes without your awareness.

The Importance of Managing Your Digital Footprint:

- Poorly managed digital footprints can lead to numerous cyber threats, including personal identity theft, fraud, personal extortion , and corporate social engineering attacks.
- Hackers often exploit the poor personal security posture of individuals to gain a foothold in corporate networks, potentially leading to data breaches and significant financial losses.
- By understanding and controlling your digital footprint, you can protect your personal information and reduce the likelihood of cyberattacks on yourself, your family, and your organization.

What is identity theft, and what are its warning signs?

Identity theft happens when someone uses your personal or financial information without your permission.

This information can include:

- Names and addresses
- Credit card or Social Security numbers
- Bank account numbers
- Medical insurance account numbers

You may not know that you experienced ID theft immediately.

Beware of these warning signs:

- Bills for items you did not buy
- Debt collection calls for accounts you did not open
- Information on your credit report for accounts you did not open
- Denials of loan applications
- Mail stops coming to or is missing from your mailbox

Plurilock CRITICAL SERVICES

Freeze Your Credit When Not Applying For Loans

Credit Reporting Agency	URL To Freeze Credit
Equifax	www.equifax.com/personal/credit-report-services
Experian	www.experian.com/freeze/center.html
TransUnion	www.transunion.com/credit-freeze

Be sure to take the time to review your credit reports on a regular basis if you are not using an automated solution to do that.

Plurilock CRITICAL SERVICES

Also, Freeze Your ChexSystems Account.

What is ChexSystems?

ChexSystems is a consumer reporting agency that helps banks decide whether to open a checking account for a new customer. They provide information for banks and credit unions much like the credit bureaus: Equifax, Experian, and TransUnion. However, there are some differences in the way they maintain and report data.

ChexSystems does not make any decisions regarding whether a bank account is opened for you. That choice depends solely on the financial institutions you decide to work with, but not all banks use ChexSystems.

As a consumer reporting agency, ChexSystems is governed by the Fair Credit Reporting Act (FCRA) and other laws enforced by the Federal Trade Commission.

This means you have access to your ChexSystems report in much the same manner as you can access the credit reports from the three major credit bureaus.

https://www.chexsystems.com/security-freeze/information

Plurilock CRITICAL SERVICES

Also, Setup an IRS identity protection personal identification number (IP PIN)

What's an IRS IP PIN?

The IRS IP PIN is a 6-digit number assigned to eligible taxpayers to help prevent the misuse of their Social Security number (SSN) on fraudulent federal income tax returns.

Anyone who has an SSN or Individual Taxpayer Identification Number (ITIN) and is able to verify his/her identity is eligible to enroll into the IP PIN program.

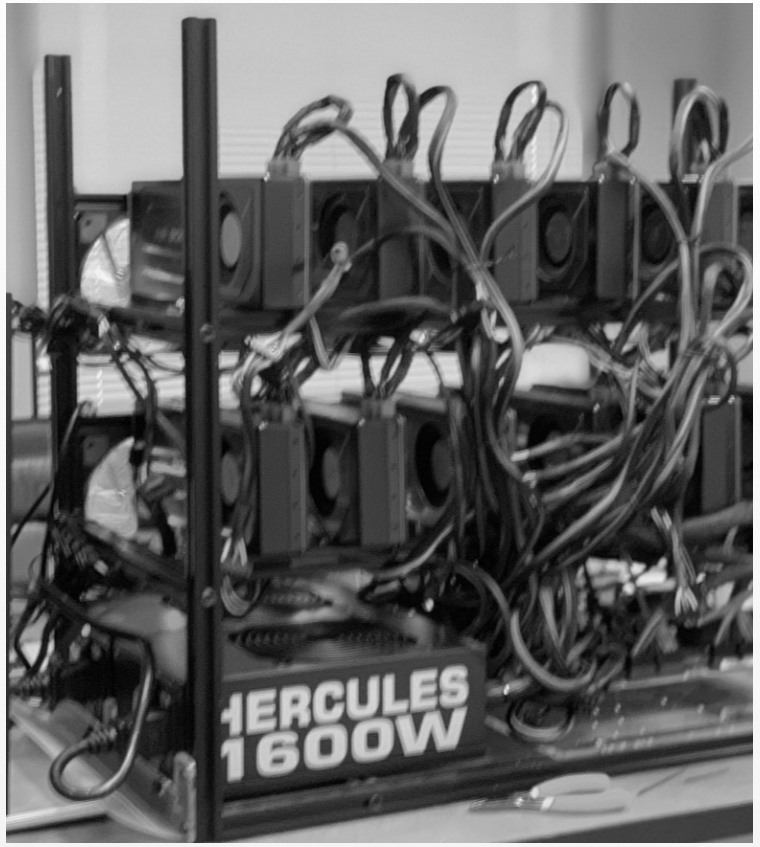
A new IP PIN will be generated each year. If the IRS assigns you an IP PIN, you must use it to confirm your identity on any return filed during the current calendar year. This includes current year returns as well as any delinquent tax returns.

An IP PIN is used only on Forms 1040, 1040-NR, 1040-PR, 1040-SR and 1040-SS.

Password Management Tips

Hackers leverage powerful dedicated graphics cards (GPUs) that can crack passwords faster than ever. In many instances hackers leverage specially built “hashing rigs” which can crack an eight-character password in less than 45 minutes.

- Use long and complex passphrases
- Utilize password managers
  - Popular password managers include 1Password, ProtonPass, KeePass, and Bitwarden.
  - Do not use your web browser to store passwords.
- Ensure MFA is used on all of your accounts
- Avoid insecure MFA methods
  - Avoid SMS, email, and OTP-based MFA as they are easier to bypass. Where possible, utilize push notification-based MFA.
- Store MFA backup codes on an offline USB Drive that’s in a secure location, do not leave them on your computer.



Note: None of the services mentioned in this presentation are sponsored by Plurilock or the author of this guide.
No warranties are provided for any of the services discussed.

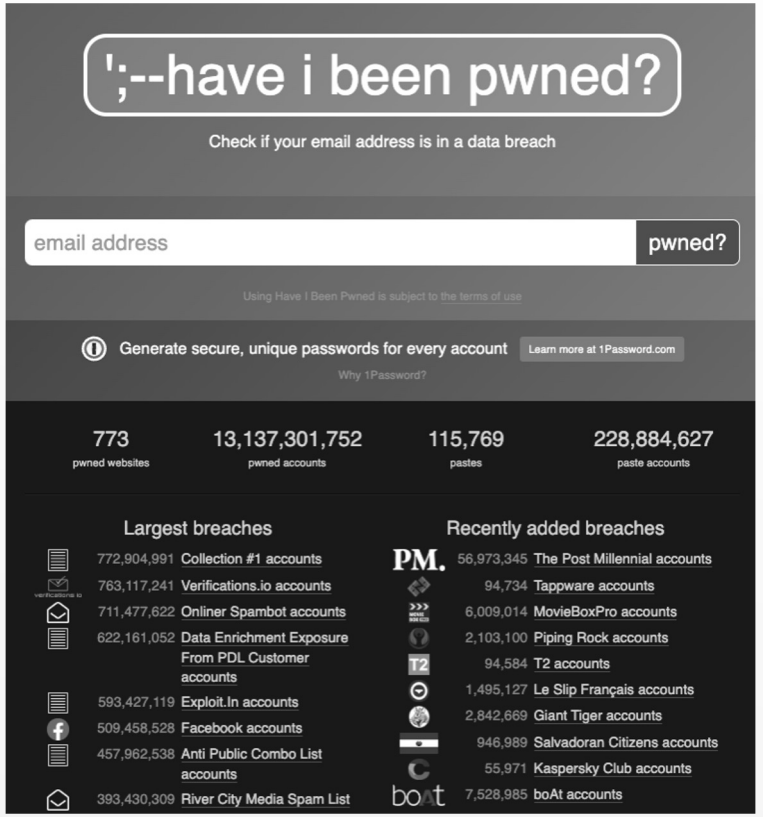
Plurilock CRITICAL SERVICES

Preventing Credential Stuffing Attacks

Free services like HaveIBeenPwned allow users to check if their email addresses or phone numbers have been compromised in any past data breaches.

By alerting users to these breaches, it enables them to change compromised passwords and enhance their online security, thus protecting them from credential stuffing attacks where attackers reuse stolen credentials to gain unauthorized access to accounts.

Setup breach notifications for your email address



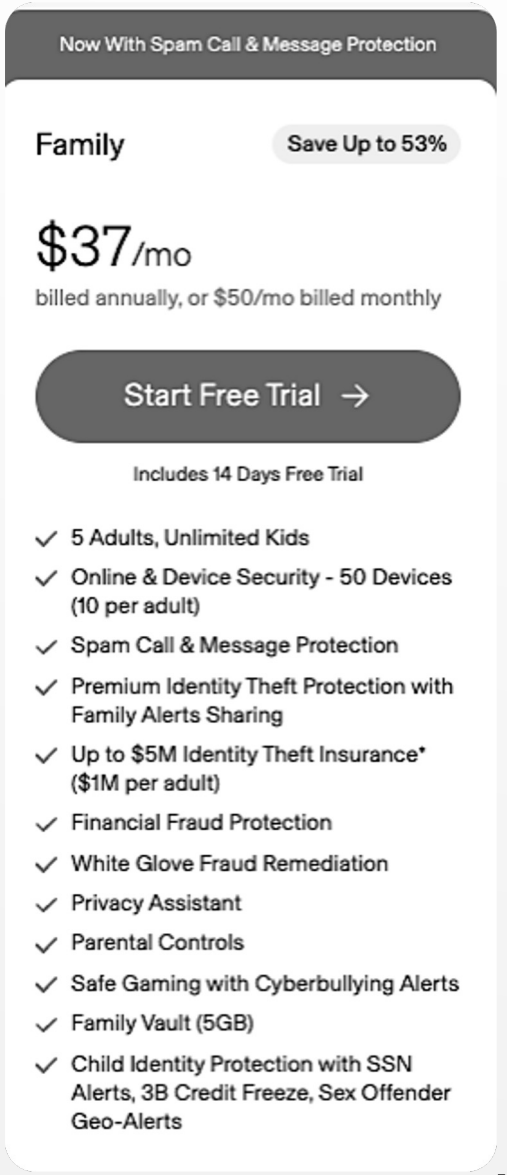
Note: None of the services mentioned in this presentation are sponsored by Plurilock or the author of this guide. No warranties are provided for any of the services discussed.

Plurilock CRITICAL SERVICES

Identity Theft Monitoring Solutions

- Leveraging Identity Theft Monitoring Solutions like Aura, LifeLock, or IDX Score can provide robust protection through continuous monitoring of your personal information and alerts for any suspicious activity.
- These services offer features such as dark web surveillance, credit report monitoring, bank account transaction monitoring, and identity restoration support, ensuring comprehensive coverage against potential threats.
- Additionally, they include identity theft insurance, providing financial reimbursement and professional assistance in the event of identity theft.

Consider leveraging an ID theft monitoring solution



Note: None of the services mentioned in this presentation are sponsored by Plurilock or the author of this guide. No warranties are provided for any of the services discussed.

Privacy Data Sanitization Services

- Hundreds of data brokers freely collect and resell records with your personal information, spreading intimate details about you across the Internet on websites like truthfinder.com, spokeo.com, intelius.com, and more.
- These sites have information like your name, age, current and previous addresses, phone numbers, info about relatives, income, etc., so it's easier than ever before to become a victim of identity theft or a VIP impersonation attack as it only takes seconds for scammers and hackers to find this personal information.

  Consider subscribing to a service that removes your personal contact information from the internet such as PrivacyBee, DeleteMe, OneRep or Aura which are affordable solutions for automatically removing your private information from the web on a recurring monthly basis.


His birth date was listed as -10-19 . Matthew was born years ago. An alternative name that Matthew can use is Matt Hil . Matthew now resides at and two other persons spent some time in this place. Address history shows that Matthew also lived at . Matthew has resided in eight places, including . Residence history shows that Matthew was associated with eight people, including . Matthew has phone numbers registered: Matthew may use the email addresses

Main Address

axh 73

County: County

FIPS: 371

Possible connections via main address -

Latitude, Longitude: 772, 288

Historical Addresses

0,

iew, CA

Phones

881 , 305 , (716)

Emails

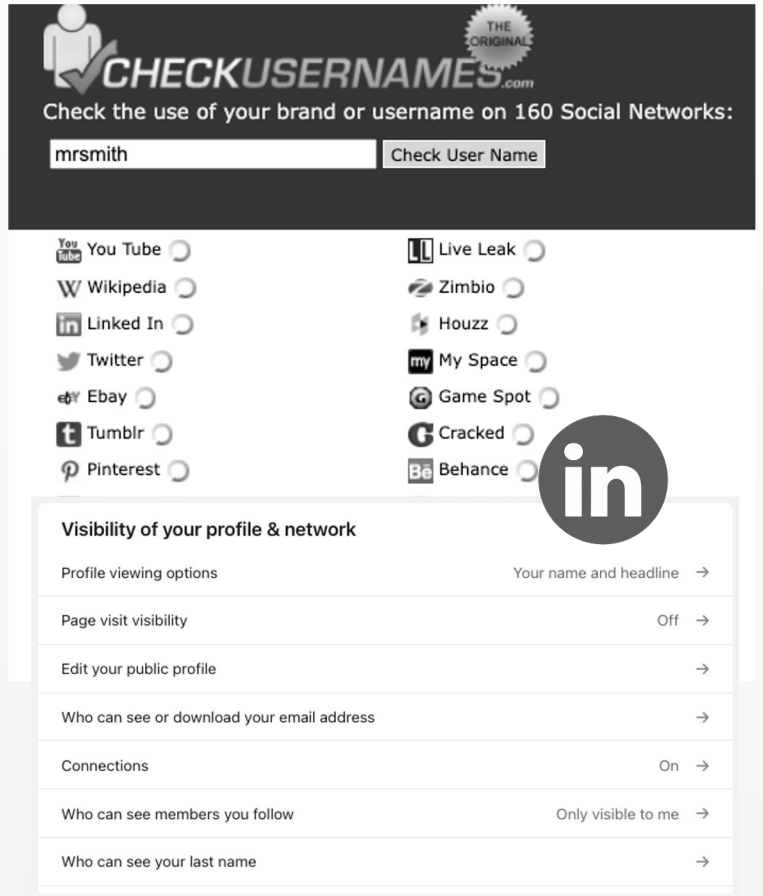
Consider leveraging privacy data sanitization services to combat data brokers

Note: None of the services mentioned in this presentation are sponsored by Plurilock or the author of this guide.
No warranties are provided for any of the services discussed.

Plurilock CRITICAL SERVICES

General Social Media Tips

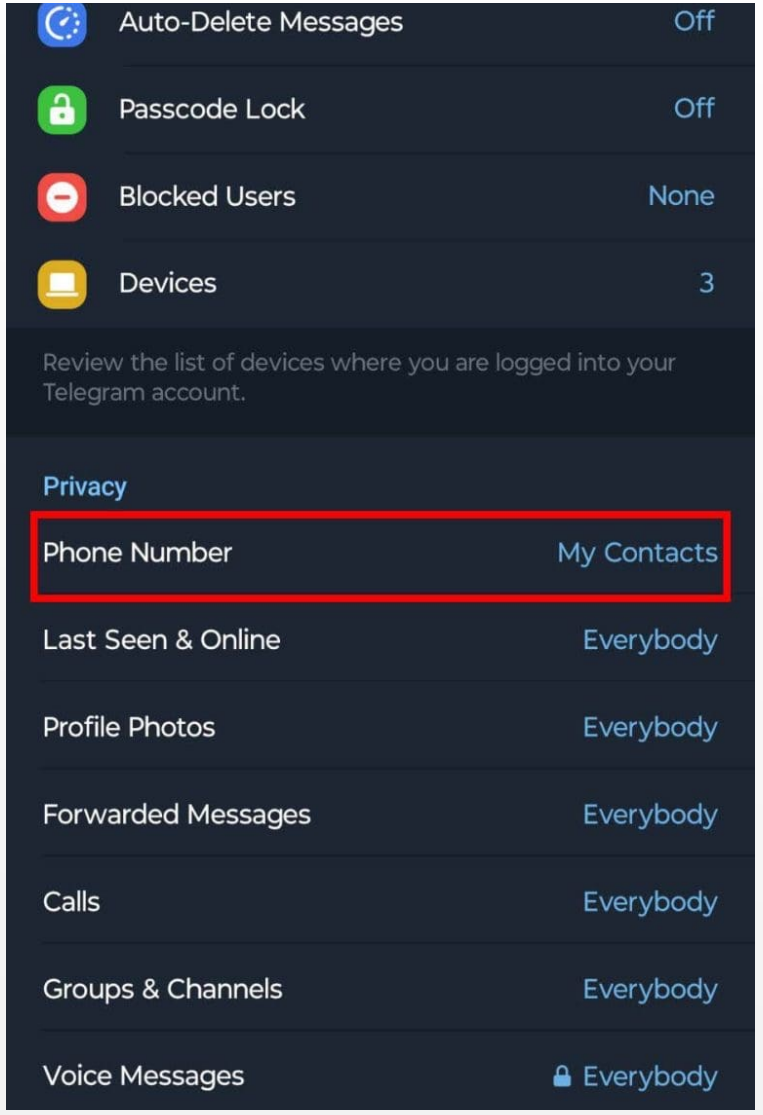
- **Minimize Personal Information**: Use only essential details like your first name and last initial on public social media sites. Consider utilizing a unique username for some sites.
- **Avoid Sharing Sensitive Details**: Do not share your home address, phone number, or other sensitive information publicly.
- **Perform Regular Privacy Reviews**: Frequently update privacy settings to control shared information.
- **Use Privacy Controls**: Limit who can see personal info such as family photos and relationship status.
- **Trusted Connections Only**: Ensure detailed personal information is accessible only to trusted connections.
- **Disable Location Sharing**: Turn off location services and be cautious of geotagged posts.



Note: None of the services mentioned in this presentation are sponsored by Plurilock or the author of this guide.
No warranties are provided for any of the services discussed.

Personal Messaging Tips

- **Use End-to-End Encrypted Apps**: Opt for apps like Signal, WhatsApp, or Telegram to ensure only you and the recipient can read your messages. Use self-destructing messages when possible.
- **Enable Two-Factor Authentication (2FA):** Use unique, strong passwords for your messaging apps and activate 2FA for an added security layer.
- **Verify Contacts**: Confirm the identity of your contacts to avoid communication with spoofed or compromised accounts.
- **Review App Permissions**: Limit app permissions to essential functions only, such as location, contacts, microphone, and camera.
- **Be Cautious with Links and Attachments**: Avoid clicking on suspicious links or downloading attachments from unknown sources.
- **Be Wary of Public Wi-Fi**: Avoid using public Wi-Fi for sensitive communications. Use a VPN if necessary.
- **Log Out of Unused Devices**: Regularly log out of devices you no longer use to prevent unauthorized access.

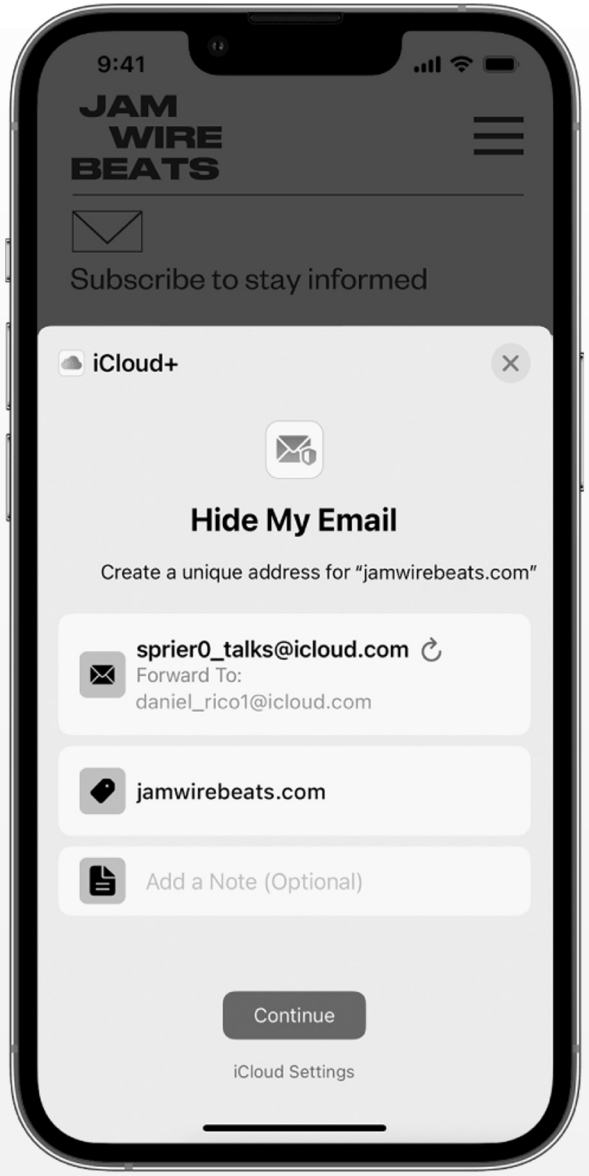


Note: None of the services mentioned in this presentation are sponsored by Plurilock or the author of this guide.
No warranties are provided for any of the services discussed.

Plurilock CRITICAL SERVICES

Enhance Your Privacy with Email Masking

- Email masking solutions, such as Apple's Hide My Email, ProtonMail, and FastMail, generate unique, random email addresses that forward messages to your real email account, helping to protect your primary email address from exposure.
- These masked emails can be used for different services and subscriptions, reducing the risk of spam and phishing attacks by keeping your actual email address private.
- While not as good, Gmail users can also create aliases by adding a "+" symbol and additional text to their main email handle, which allows them to filter and manage incoming emails more effectively, further enhancing security. For example, jsmith@gmail.com you could use an alias like jsmith+news@gmail.com.
- Utilize email masking solutions, especially for less trusted websites or public emails



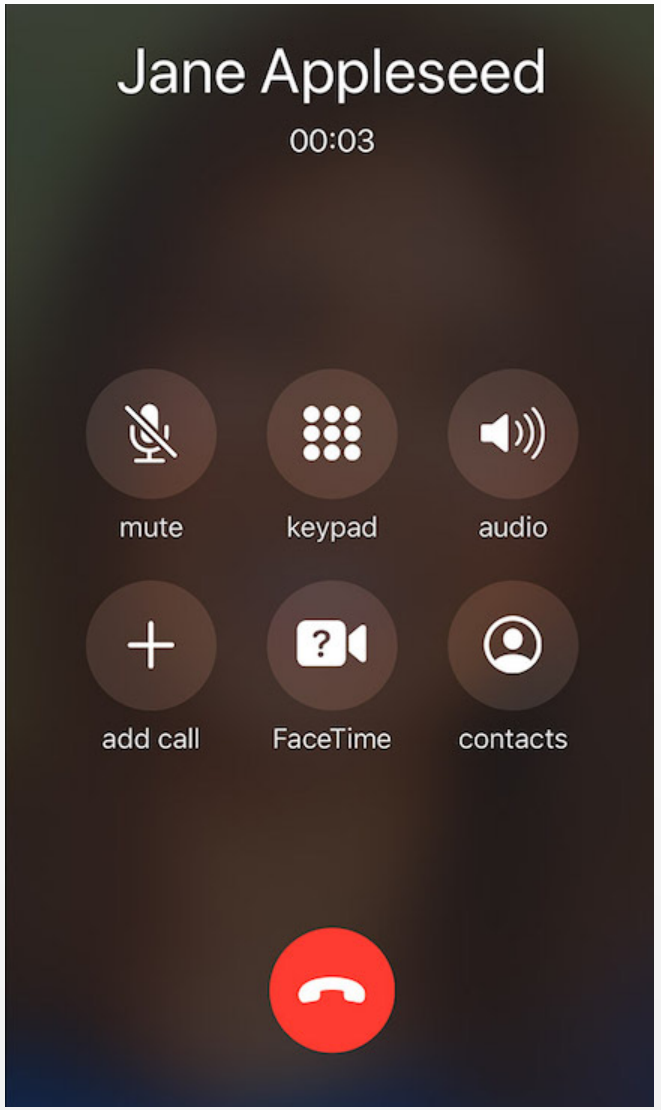
Note: None of the services mentioned in this presentation are sponsored by Plurilock or the author of this guide.
No warranties are provided for any of the services discussed.

Phone Call Screening

- Phone call screening apps help identify and block spam and fraudulent calls, protecting you from potential scams and phishing attempts.
- Many screening apps allow you to create custom block lists and provide detailed caller ID information, giving you control over who can reach you and how your calls are managed.
- Leverage a phone call screening solution
- Be mindful that hackers can spoof phone numbers

Some solutions include:

- Verizon Call Filter
- T-Mobile Scam Shield
- AT&T ActiveArmor
- O2 Call Protect
- Vodafone Secure Net



Note: None of the services mentioned in this presentation are sponsored by Plurilock or the author of this guide.
No warranties are provided for any of the services discussed.

Preventing SIM Swapping Attacks

A SIM swap attack (also known as SIM porting or SIM hijacking) occurs when an attacker tricks a mobile phone service provider into transferring a customer's phone number to the attacker's SIM card, enabling them to intercept calls and text messages, including verification codes.

To thwart SIM swapping, set up a SIM Security PIN with your carrier, which adds an extra layer of security before any changes can be made to your account.

SIM Security Pin Instructions:

Common USA Cellular Providers

- AT&T
- Verizon
- T-Mobile

Common UK Cellular Providers

- EE
- Vodafone
- O2

Note: None of the services mentioned in this presentation are sponsored by Plurilock or the author of this guide.
No warranties are provided for any of the services discussed.

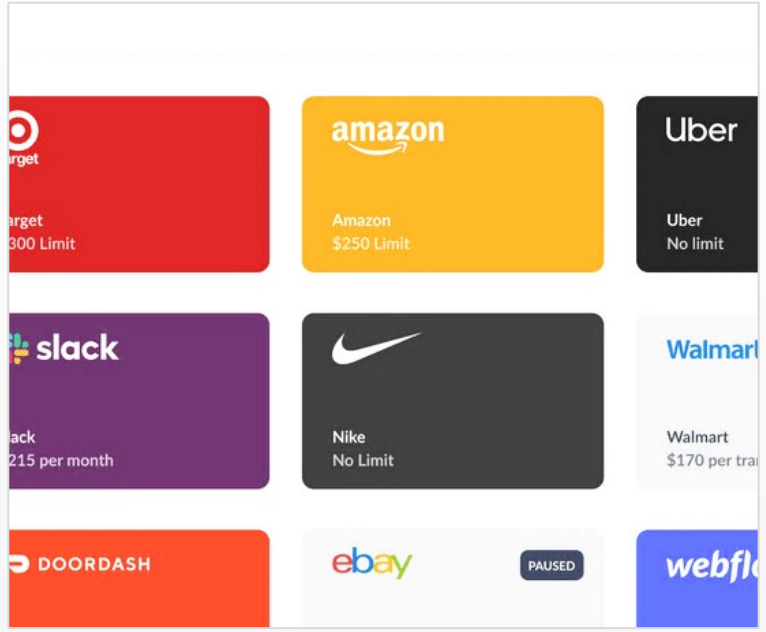
Plurilock CRITICAL SERVICES

Utilizing Virtual Cards For Online Shopping

Services like Privacy.com and Zen.com provide virtual cards that can be used for online purchases.

Virtual cards function just like real credit or debit cards but without physical cards and can be used for online shopping, over-the-phone purchases, or any transaction that requires entering a card number.

These virtual card numbers limit your exposure by masking the real card information, thereby reducing the risk of fraud and unauthorized charges to your bank accounts.



Consider Utilizing Virtual Cards

Note: None of the services mentioned in this presentation are sponsored by Plurilock or the author of this guide. No warranties are provided for any of the services discussed.

Plurilock CRITICAL SERVICES

Reducing Your Personal Attack Surface

Summary

- Freeze your credit
- Freeze ChexSystems
- Set up an IRS IP pin
- Practice proactive password management
- Set up ID theft monitoring
- Sanitize your information from data broker sites
- Harden your social media accounts
- Secure messaging, phone & email communications
- Prevent SIM swapping attacks
- Prevent credit/debit card breaches

Plurilock
CRITICAL SERVICES

About Plurilock™

Plurilock
CRITICAL SERVICES

Advanced Consulting for Critical Business Problems

Plurilock Critical Services delivers the expertise and capabilities you need in a world of increasing risk—quickly.

- **IP Protection (IP3)**
  insider threat ▪ DLP ▪ CASB ▪ data encryption ▪ cloud security ▪ IP processes and contracts
- **Zero Trust (ZTP)**
  cloud ▪ networking ▪ firewalls ▪ VPN ▪ network segmentation
- **Offensive Security (OffSec)**
  pentesting ▪ red teaming ▪ vulnerability research
- **Security Operations (SecOps)**
  threat intelligence ▪ security engineering ▪ SIEM
- **Advisory (AP)**
  compliance assessments (SOC 1 and 2, ISO 27001, CMMC, NIST and NIST CSF, PCI, MITRE) ▪ AI risk management

Who We Are

Plurilock is an enterprise provider with the experience, expertise, and resources to provide end-to-end solutions to the most intractable problems in enterprise IT.

- **World-class research, engineering**
  Founded as a research spinout, Plurilock boasts multiple patents, PhD scientists and engineers, and its own comprehensive line of cybersecurity products.
- **World-class field expertise**
  Our veteran team of battle-tested technology, platform, and vendor field engineers holds some of the world's most exclusive certifications.
- **We offer what others can't**
  One team that handles every part of the solution, from discussion and ideation through procurement and successful deployment and integration.

Selection of current and past Plurilock family customers

Talk to Plurilock ▪ sales@plurilock.com ▪ plurilock.com/cs/

Plurilock
CRITICAL SERVICES