Protecting Research Integrity with Secure Data and Communication Practices

Why Data Privacy Matters

Why Data Privacy Matters

- Behavioral research often involves private data and even experimental results can be highly sensitive

Why Data Privacy Matters

- Behavioral research often involves private data and even experimental results can be highly sensitive
- Even seemingly innocuous data can be a tool of abuse

Why Data Privacy Matters

- Behavioral research often involves private data and even experimental results can be highly sensitive
- Even seemingly innocuous data can be a tool of abuse
  - an employer might take adverse action against an employee based on their scores in an implicit bias test, or responses to a survey on political attitudes, or sexual preference, or ...

Why Data Privacy Matters

- Behavioral research often involves private data and even experimental results can be highly sensitive
- Even seemingly innocuous data can be a tool of abuse
  - an employer might take adverse action against an employee based on their scores in an implicit bias test, or responses to a survey on political attitudes, or sexual preference, or ...
- Data privacy can be a matter of life and death

Why Data Privacy Matters

- Behavioral research often involves private data and even experimental results can be highly sensitive
- Even seemingly innocuous data can be a tool of abuse
  - an employer might take adverse action against an employee based on their scores in an implicit bias test, or responses to a survey on political attitudes, or sexual preference, or ...
- Data privacy can be a matter of life and death
  - imagine that your research subjects are domestic abuse victims, or undocumented residents, or political dissidents, or mafia informants, or ...

Why Data Privacy Matters

- Behavioral research often involves private data and even experimental results can be highly sensitive
- Even seemingly innocuous data can be a tool of abuse
  - an employer might take adverse action against an employee based on their scores in an implicit bias test, or responses to a survey on political attitudes, or sexual preference, or ...
- Data privacy can be a matter of life and death
  - imagine that your research subjects are domestic abuse victims, or undocumented residents, or political dissidents, or mafia informants, or ...
- With most data stored and transmitted digitally, researchers should take security measures proactively

Data privacy

Why Data Privacy Matters

Psychologists have a primary obligation and take reasonable precautions to protect confidential information obtained through or stored in any medium, recognizing that the extent and limits of confidentiality may be regulated by law or established by institutional rules or professional or scientific relationship.

— APA Standard 4.01 (“Maintaining Confidentiality”)

Why Data Privacy Matters

- Data privacy obligations are both legal and ethical, but also practical:

Why Data Privacy Matters

- Data privacy obligations are both legal and ethical, but also practical:
  - secure practices build trust with participants, collaborators, and funding agencies, and other stakeholders

Why Data Privacy Matters

- Data privacy obligations are both legal and ethical, but also practical:
  - secure practices build trust with participants, collaborators, and funding agencies, and other stakeholders
- Ethical and practical considerations go far beyond legal obligation!

Why Data Privacy Matters

- Data privacy obligations are both legal and ethical, but also practical:
  - secure practices build trust with participants, collaborators, and funding agencies, and other stakeholders
- Ethical and practical considerations go far beyond legal obligation!
  - it is possible to follow the law perfectly and still run the risk of inviting harassment of research subjects, or embarrassing yourself, your colleagues, your participants, your employer ...

Why Data Privacy Matters

- Data privacy obligations are both legal and ethical, but also practical:
  - secure practices build trust with participants, collaborators, and funding agencies, and other stakeholders
- Ethical and practical considerations go far beyond legal obligation!
  - it is possible to follow the law perfectly and still run the risk of inviting harassment of research subjects, or embarrassing yourself, your colleagues, your participants, your employer ...
  - most employers will help you follow the law

Why Data Privacy Matters

- Data privacy obligations are both legal and ethical, but also practical:
  - secure practices build trust with participants, collaborators, and funding agencies, and other stakeholders
- Ethical and practical considerations go far beyond legal obligation!
  - it is possible to follow the law perfectly and still run the risk of inviting harassment of research subjects, or embarrassing yourself, your colleagues, your participants, your employer ...
  - most employers will help you follow the law

For further insights, see the EFF Privacy page and Privacy Tools.

Deidentification of Human Subjects Data

- By law, we must protect participant privacy (HIPAA, GDPR)

Deidentification of Human Subjects Data

- By law, we must protect participant privacy (HIPAA, GDPR)
- But we are also expected to share and publish research data

Deidentification of Human Subjects Data

- By law, we must protect participant privacy (HIPAA, GDPR)
- But we are also expected to share and publish research data
- Standard data preprocessing includes deidentification:

Deidentification of Human Subjects Data

- By law, we must protect participant privacy (HIPAA, GDPR)
- But we are also expected to share and publish research data
- Standard data preprocessing includes deidentification:
  - remove identifiers (names, social security numbers, phone numbers, etc.)

Deidentification of Human Subjects Data

- By law, we must protect participant privacy (HIPAA, GDPR)
- But we are also expected to share and publish research data
- Standard data preprocessing includes deidentification:
  - remove identifiers (names, social security numbers, phone numbers, etc.)
  - pseudonymization, data masking (synthetic or 'notional' data)

Deidentification of Human Subjects Data

- By law, we must protect participant privacy (HIPAA, GDPR)
- But we are also expected to share and publish research data
- Standard data preprocessing includes deidentification:
  - remove identifiers (names, social security numbers, phone numbers, etc.)
  - pseudonymization, data masking (synthetic or 'notional' data)
  - unlink and aggregate data when possible

Deidentification of Human Subjects Data

- By law, we must protect participant privacy (HIPAA, GDPR)
- But we are also expected to share and publish research data
- Standard data preprocessing includes deidentification:
  - remove identifiers (names, social security numbers, phone numbers, etc.)
  - pseudonymization, data masking (synthetic or 'notional' data)
  - unlink and aggregate data when possible
- There is often a residual risk of re-identification (especially with multidimensional, linked data)

Deidentification of Human Subjects Data

- By law, we must protect participant privacy (HIPAA, GDPR)
- But we are also expected to share and publish research data
- Standard data preprocessing includes deidentification:
  - remove identifiers (names, social security numbers, phone numbers, etc.)
  - pseudonymization, data masking (synthetic or 'notional' data)
  - unlink and aggregate data when possible
- There is often a residual risk of re-identification (especially with multidimensional, linked data)
- There exist established guidelines (e.g., from HHS)

Deidentification of Human Subjects Data

- By law, we must protect participant privacy (HIPAA, GDPR)
- But we are also expected to share and publish research data
- Standard data preprocessing includes deidentification:
  - remove identifiers (names, social security numbers, phone numbers, etc.)
  - pseudonymization, data masking (synthetic or 'notional' data)
  - unlink and aggregate data when possible
- There is often a residual risk of re-identification (especially with multidimensional, linked data)
- There exist established guidelines (e.g., from HHS)

  See: HIPAA De-identification Guidelines

Threat model approach

Threat Model Approach

Once again I believe that computer science holds relevant lessons for practical cognitive science.

Threat Model Approach

Once again I believe that computer science holds relevant lessons for practical cognitive science.

- Cybersecurity involves threat model analysis

Threat Model Approach

Once again I believe that computer science holds relevant lessons for practical cognitive science.

- Cybersecurity involves threat model analysis
  - structured way to identify and mitigate potential security risks

Threat Model Approach

Once again I believe that computer science holds relevant lessons for practical cognitive science.

- Cybersecurity involves threat model analysis
  - structured way to identify and mitigate potential security risks
  - carefully consider who might try to access your data and why

Threat Model Approach

Once again I believe that computer science holds relevant lessons for practical cognitive science.

- Cybersecurity involves threat model analysis
  - structured way to identify and mitigate potential security risks
  - carefully consider who might try to access your data and why
- Basic threat models:

Threat Model Approach

Once again I believe that computer science holds relevant lessons for practical cognitive science.

- Cybersecurity involves threat model analysis
  - structured way to identify and mitigate potential security risks
  - carefully consider who might try to access your data and why
- Basic threat models:
  - insider threats: actions by trusted individuals

Threat Model Approach

Once again I believe that computer science holds relevant lessons for practical cognitive science.

- Cybersecurity involves threat model analysis
  - structured way to identify and mitigate potential security risks
  - carefully consider who might try to access your data and why
- Basic threat models:
  - insider threats: actions by trusted individuals
  - external threats: hackers, adversaries, state-sponsored entities

Threat Model Approach

Once again I believe that computer science holds relevant lessons for practical cognitive science.

- Cybersecurity involves threat model analysis
  - structured way to identify and mitigate potential security risks
  - carefully consider who might try to access your data and why
- Basic threat models:
  - insider threats: actions by trusted individuals
  - external threats: hackers, adversaries, state-sponsored entities
  - accidental exposure: misconfigurations, inadvertent data leaks

Threat Model Approach

Once again I believe that computer science holds relevant lessons for practical cognitive science.

- Cybersecurity involves threat model analysis
  - structured way to identify and mitigate potential security risks
  - carefully consider who might try to access your data and why
- Basic threat models:
  - insider threats: actions by trusted individuals
  - external threats: hackers, adversaries, state-sponsored entities
  - accidental exposure: misconfigurations, inadvertent data leaks
- Goal is to assess impact and likelihood of potential attack vectors and tailor security policies based on your threat profile

Threat Model Approach

Once again I believe that computer science holds relevant lessons for practical cognitive science.

- Cybersecurity involves threat model analysis
  - structured way to identify and mitigate potential security risks
  - carefully consider who might try to access your data and why
- Basic threat models:
  - insider threats: actions by trusted individuals
  - external threats: hackers, adversaries, state-sponsored entities
  - accidental exposure: misconfigurations, inadvertent data leaks
- Goal is to assess impact and likelihood of potential attack vectors and tailor security policies based on your threat profile

For more details, see the NIST Threat Modeling Guidelines.

Threat Model Analysis: An Abstract Overview

Threat Model Analysis: An Abstract Overview

1. Identify assets

Threat Model Analysis: An Abstract Overview

1. Identify assets
    - What valuable information or resources need protection?

Threat Model Analysis: An Abstract Overview

1. Identify assets
    - What valuable information or resources need protection?
      Sensitive data, intellectual property, personal identities...

Threat Model Analysis: An Abstract Overview

1. Identify assets
   - What valuable information or resources need protection?
     Sensitive data, intellectual property, personal identities...
2. Identify potential adversaries

Threat Model Analysis: An Abstract Overview

1. Identify assets
   - What valuable information or resources need protection?
     Sensitive data, intellectual property, personal identities...
2. Identify potential adversaries
   - Who might target your assets?

Threat Model Analysis: An Abstract Overview

1. Identify assets
   - What valuable information or resources need protection?
     Sensitive data, intellectual property, personal identities...
2. Identify potential adversaries
   - Who might target your assets?
     External attackers, insiders, or opportunistic threats.

Threat Model Analysis: An Abstract Overview

1. Identify assets
   - What valuable information or resources need protection?
     Sensitive data, intellectual property, personal identities...
2. Identify potential adversaries
   - Who might target your assets?
     External attackers, insiders, or opportunistic threats.
3. Determine threat vectors

Threat Model Analysis: An Abstract Overview

1. Identify assets
   - What valuable information or resources need protection?
     Sensitive data, intellectual property, personal identities...
2. Identify potential adversaries
   - Who might target your assets?
     External attackers, insiders, or opportunistic threats.
3. Determine threat vectors
   - How could adversaries attack?

Threat Model Analysis: An Abstract Overview

1. Identify assets
   - What valuable information or resources need protection?
     Sensitive data, intellectual property, personal identities...
2. Identify potential adversaries
   - Who might target your assets?
     External attackers, insiders, or opportunistic threats.
3. Determine threat vectors
   - How could adversaries attack?
     Look at digital channels (e.g., network intrusions) and physical or social channels (e.g., social engineering).

Threat Model Analysis: An Abstract Overview

1. Identify assets
   - What valuable information or resources need protection?
     Sensitive data, intellectual property, personal identities...
2. Identify potential adversaries
   - Who might target your assets?
     External attackers, insiders, or opportunistic threats.
3. Determine threat vectors
   - How could adversaries attack?
     Look at digital channels (e.g., network intrusions) and physical or social channels (e.g., social engineering).
4. Assess impact and likelihood

Threat Model Analysis: An Abstract Overview

1. Identify assets
   - What valuable information or resources need protection?
     Sensitive data, intellectual property, personal identities...
2. Identify potential adversaries
   - Who might target your assets?
     External attackers, insiders, or opportunistic threats.
3. Determine threat vectors
   - How could adversaries attack?
     Look at digital channels (e.g., network intrusions) and physical or social channels (e.g., social engineering).
4. Assess impact and likelihood
   - How severe is a potential breach and how likely is it?

Threat Model Analysis: An Abstract Overview

1. Identify assets
   - What valuable information or resources need protection?
     Sensitive data, intellectual property, personal identities...
2. Identify potential adversaries
   - Who might target your assets?
     External attackers, insiders, or opportunistic threats.
3. Determine threat vectors
   - How could adversaries attack?
     Look at digital channels (e.g., network intrusions) and physical or social channels (e.g., social engineering).
4. Assess impact and likelihood
   - How severe is a potential breach and how likely is it?
     E.g., how skilled are the adversaries?

5. Evaluate vulnerabilities

Threat Model Analysis: An Abstract Overview

5. Evaluate vulnerabilities
    - Where are the weak points?

5. Evaluate vulnerabilities
   - Where are the weak points?
     Assess system weaknesses, communication channels, and human factors.

Threat Model Analysis: An Abstract Overview

5. Evaluate vulnerabilities
    - Where are the weak points?
      Assess system weaknesses, communication channels, and human factors.
6. Develop mitigation strategies

Threat Model Analysis: An Abstract Overview

5. Evaluate vulnerabilities
   - Where are the weak points?
     Assess system weaknesses, communication channels, and human factors.
6. Develop mitigation strategies
   - What measures can reduce risk?

Threat Model Analysis: An Abstract Overview

5. Evaluate vulnerabilities
   - Where are the weak points?
     Assess system weaknesses, communication channels, and human factors.
6. Develop mitigation strategies
   - What measures can reduce risk?
     Consider encryption, access controls, secure practices, and training.

Threat Model Analysis: An Abstract Overview

5. Evaluate vulnerabilities
   - Where are the weak points?
     Assess system weaknesses, communication channels, and human factors.
6. Develop mitigation strategies
   - What measures can reduce risk?
     Consider encryption, access controls, secure practices, and training.
7. Frequently iterate and update

Threat Model Analysis: An Abstract Overview

5. Evaluate vulnerabilities
   - Where are the weak points?
     Assess system weaknesses, communication channels, and human factors.
6. Develop mitigation strategies
   - What measures can reduce risk?
     Consider encryption, access controls, secure practices, and training.
7. Frequently iterate and update
   - Regularly revisit your threat model as conditions change.

Threat Model Analysis: An Abstract Overview

Let's consider two cognitive scientists:

Threat Model Analysis: An Abstract Overview

Let's consider two cognitive scientists:

- Ash is a researcher at the NIJ who studies mafia informants.

Threat Model Analysis: An Abstract Overview

Let's consider two cognitive scientists:

- Ash is a researcher at the NIJ who studies mafia informants.
- Blake is a researcher at the ACLU who corresponds with dissidents in an autocratic foreign regime.

Threat Model: Studying Mafia Informants

Assets

Threat Model: Studying Mafia Informants

Assets

- *Research Data:* Sensitive documents, interview recordings, and field notes.

Threat Model: Studying Mafia Informants

Assets

- *Research Data:* Sensitive documents, interview recordings, and field notes.
- *Informant Anonymity:* Identities and contact details of sources.

Threat Model: Studying Mafia Informants

Assets

- *Research Data:* Sensitive documents, interview recordings, and field notes.
- *Informant Anonymity:* Identities and contact details of sources.
- *Personal Safety & Reputation:* The researcher's well-being and academic credibility.

Threat Model: Studying Mafia Informants

Assets

- *Research Data:* Sensitive documents, interview recordings, and field notes.
- *Informant Anonymity:* Identities and contact details of sources.
- *Personal Safety & Reputation:* The researcher's well-being and academic credibility.

Adversaries

Threat Model: Studying Mafia Informants

Assets

- *Research Data:* Sensitive documents, interview recordings, and field notes.
- *Informant Anonymity:* Identities and contact details of sources.
- *Personal Safety & Reputation:* The researcher's well-being and academic credibility.

Adversaries

- *Criminal Organizations:* Mafia groups aiming to suppress negative information and to identify informants.

Threat Model: Studying Mafia Informants

Assets

- *Research Data:* Sensitive documents, interview recordings, and field notes.
- *Informant Anonymity:* Identities and contact details of sources.
- *Personal Safety & Reputation:* The researcher's well-being and academic credibility.

Adversaries

- *Criminal Organizations:* Mafia groups aiming to suppress negative information and to identify informants.
- *Corrupt Actors:* Individuals within law enforcement with ties to organized crime.

Threat Model: Studying Mafia Informants

Assets

- *Research Data:* Sensitive documents, interview recordings, and field notes.
- *Informant Anonymity:* Identities and contact details of sources.
- *Personal Safety & Reputation:* The researcher's well-being and academic credibility.

Adversaries

- *Criminal Organizations:* Mafia groups aiming to suppress negative information and to identify informants.
- *Corrupt Actors:* Individuals within law enforcement with ties to organized crime.
- *Insider Threats:* Untrusted collaborators or assistants.

Threat Model: Studying Mafia Informants

Threat vectors

Threat Model: Studying Mafia Informants

Threat vectors

- Digital surveillance (hacking emails, cloud storage, etc.)

Threat Model: Studying Mafia Informants

Threat vectors

- Digital surveillance (hacking emails, cloud storage, etc.)
- Physical intrusion (unauthorized access to devices or facilities)

Threat Model: Studying Mafia Informants

Threat vectors

- Digital surveillance (hacking emails, cloud storage, etc.)
- Physical intrusion (unauthorized access to devices or facilities)
- Social engineering (coercion or manipulation)

Threat Model: Studying Mafia Informants

Threat vectors

- Digital surveillance (hacking emails, cloud storage, etc.)
- Physical intrusion (unauthorized access to devices or facilities)
- Social engineering (coercion or manipulation)

Vulnerabilities

Threat Model: Studying Mafia Informants

Threat vectors

- Digital surveillance (hacking emails, cloud storage, etc.)
- Physical intrusion (unauthorized access to devices or facilities)
- Social engineering (coercion or manipulation)

Vulnerabilities

- Insecure communications (lack of encryption)

Threat Model: Studying Mafia Informants

Threat vectors

- Digital surveillance (hacking emails, cloud storage, etc.)
- Physical intrusion (unauthorized access to devices or facilities)
- Social engineering (coercion or manipulation)

Vulnerabilities

- Insecure communications (lack of encryption)
- Data storage risks (unencrypted local storage)

Threat Model: Studying Mafia Informants

Threat vectors

- Digital surveillance (hacking emails, cloud storage, etc.)
- Physical intrusion (unauthorized access to devices or facilities)
- Social engineering (coercion or manipulation)

Vulnerabilities

- Insecure communications (lack of encryption)
- Data storage risks (unencrypted local storage)
- Operational security gaps (lack of staff cybersecurity training; failure to deidentify informant data)

Threat Model: Studying Mafia Informants

Threat vectors

- Digital surveillance (hacking emails, cloud storage, etc.)
- Physical intrusion (unauthorized access to devices or facilities)
- Social engineering (coercion or manipulation)

Vulnerabilities

- Insecure communications (lack of encryption)
- Data storage risks (unencrypted local storage)
- Operational security gaps (lack of staff cybersecurity training; failure to deidentify informant data)

Mitigations

Threat Model: Studying Mafia Informants

Threat vectors

- Digital surveillance (hacking emails, cloud storage, etc.)
- Physical intrusion (unauthorized access to devices or facilities)
- Social engineering (coercion or manipulation)

Vulnerabilities

- Insecure communications (lack of encryption)
- Data storage risks (unencrypted local storage)
- Operational security gaps (lack of staff cybersecurity training; failure to deidentify informant data)

Mitigations

- Use robust encryption (for communications and data storage)

Threat Model: Studying Mafia Informants

Threat vectors

- Digital surveillance (hacking emails, cloud storage, etc.)
- Physical intrusion (unauthorized access to devices or facilities)
- Social engineering (coercion or manipulation)

Vulnerabilities

- Insecure communications (lack of encryption)
- Data storage risks (unencrypted local storage)
- Operational security gaps (lack of staff cybersecurity training; failure to deidentify informant data)

Mitigations

- Use robust encryption (for communications and data storage)
- Strong deidentification and pseudonymization procedures

Threat Model: Studying Mafia Informants

Threat vectors

- Digital surveillance (hacking emails, cloud storage, etc.)
- Physical intrusion (unauthorized access to devices or facilities)
- Social engineering (coercion or manipulation)

Vulnerabilities

- Insecure communications (lack of encryption)
- Data storage risks (unencrypted local storage)
- Operational security gaps (lack of staff cybersecurity training; failure to deidentify informant data)

Mitigations

- Use robust encryption (for communications and data storage)
- Strong deidentification and pseudonymization procedures
- Enforce staff training in operational security (OpSec)

Threat Model: Studying Mafia Informants

Threat vectors

- Digital surveillance (hacking emails, cloud storage, etc.)
- Physical intrusion (unauthorized access to devices or facilities)
- Social engineering (coercion or manipulation)

Vulnerabilities

- Insecure communications (lack of encryption)
- Data storage risks (unencrypted local storage)
- Operational security gaps (lack of staff cybersecurity training; failure to deidentify informant data)

Mitigations

- Use robust encryption (for communications and data storage)
- Strong deidentification and pseudonymization procedures
- Enforce staff training in operational security (OpSec)
- Limit access to sensitive data on a need-to-know basis

Threat Model: Studying Mafia Informants

Threat vectors

- Digital surveillance (hacking emails, cloud storage, etc.)
- Physical intrusion (unauthorized access to devices or facilities)
- Social engineering (coercion or manipulation)

Vulnerabilities

- Insecure communications (lack of encryption)
- Data storage risks (unencrypted local storage)
- Operational security gaps (lack of staff cybersecurity training; failure to deidentify informant data)

Mitigations

- Use robust encryption (for communications and data storage)
- Strong deidentification and pseudonymization procedures
- Enforce staff training in operational security (OpSec)
- Limit access to sensitive data on a need-to-know basis
- Does the data need to be transmitted at all?

Threat Model: Studying Mafia Informants

Encryption tools

Threat Model: Studying Mafia Informants

Encryption tools

- GnuPG/PGP for secure email and file encryption.

Threat Model: Studying Mafia Informants

Encryption tools

- GnuPG/PGP for secure email and file encryption.
- VeraCrypt for full-disk or volume encryption.

Threat Model: Studying Mafia Informants

Encryption tools

- GnuPG/PGP for secure email and file encryption.
- VeraCrypt for full-disk or volume encryption.
- Python cryptography library for custom data encryption.

Threat Model: Studying Mafia Informants

Encryption tools

- GnuPG/PGP for secure email and file encryption.
- VeraCrypt for full-disk or volume encryption.
- Python cryptography library for custom data encryption.

Secure communications

Threat Model: Studying Mafia Informants

Encryption tools

- GnuPG/PGP for secure email and file encryption.
- VeraCrypt for full-disk or volume encryption.
- Python cryptography library for custom data encryption.

Secure communications

- Signal for end-to-end encrypted messaging.

Threat Model: Studying Mafia Informants

Encryption tools

- GnuPG/PGP for secure email and file encryption.
- VeraCrypt for full-disk or volume encryption.
- Python cryptography library for custom data encryption.

Secure communications

- Signal for end-to-end encrypted messaging.
- ProtonMail for secure, encrypted email.

Threat Model: Studying Mafia Informants

Encryption tools

- GnuPG/PGP for secure email and file encryption.
- VeraCrypt for full-disk or volume encryption.
- Python cryptography library for custom data encryption.

Secure communications

- Signal for end-to-end encrypted messaging.
- ProtonMail for secure, encrypted email.
- Use encrypted collaboration platforms such as Wire.

Threat Model: Studying Mafia Informants

Encryption tools

- GnuPG/PGP for secure email and file encryption.
- VeraCrypt for full-disk or volume encryption.
- Python cryptography library for custom data encryption.

Secure communications

- Signal for end-to-end encrypted messaging.
- ProtonMail for secure, encrypted email.
- Use encrypted collaboration platforms such as Wire.

Threat Model: Studying Mafia Informants

Encryption tools

- GnuPG/PGP for secure email and file encryption.
- VeraCrypt for full-disk or volume encryption.
- Python cryptography library for custom data encryption.

Secure communications

- Signal for end-to-end encrypted messaging.
- ProtonMail for secure, encrypted email.
- Use encrypted collaboration platforms such as Wire.

There's really no reason you couldn't use all of these tools routinely. They work! ChatGPT will tell you how to install them.

Threat Model: Studying Mafia Informants

Network and data security

Threat Model: Studying Mafia Informants

Network and data security

- Use reputable VPN services (e.g., NordVPN, ProtonVPN, ExpressVPN) to secure internet traffic.

Threat Model: Studying Mafia Informants

Network and data security

- Use reputable VPN services (e.g., NordVPN, ProtonVPN, ExpressVPN) to secure internet traffic.
- Run DNS leak tests with services like dnsleaktest.com.

Threat Model: Studying Mafia Informants

Network and data security

- Use reputable VPN services (e.g., NordVPN, ProtonVPN, ExpressVPN) to secure internet traffic.
- Run DNS leak tests with services like dnsleaktest.com.
- Use secure cloud storage options such as SpiderOak or Tresorit.

Threat Model: Studying Mafia Informants

Network and data security

- Use reputable VPN services (e.g., NordVPN, ProtonVPN, ExpressVPN) to secure internet traffic.
- Run DNS leak tests with services like dnsleaktest.com.
- Use secure cloud storage options such as SpiderOak or Tresorit.

Operational security

Threat Model: Studying Mafia Informants

Network and data security

- Use reputable VPN services (e.g., NordVPN, ProtonVPN, ExpressVPN) to secure internet traffic.
- Run DNS leak tests with services like dnsleaktest.com.
- Use secure cloud storage options such as SpiderOak or Tresorit.

Operational security

- Enforce two-factor authentication (2FA) using tools like Authy or Google Authenticator.

Threat Model: Studying Mafia Informants

Network and data security

- Use reputable VPN services (e.g., NordVPN, ProtonVPN, ExpressVPN) to secure internet traffic.
- Run DNS leak tests with services like dnsleaktest.com.
- Use secure cloud storage options such as SpiderOak or Tresorit.

Operational security

- Enforce two-factor authentication (2FA) using tools like Authy or Google Authenticator.
- Staff cybersecurity training and phishing awareness sessions.

Threat Model: Studying Mafia Informants

Network and data security

- Use reputable VPN services (e.g., NordVPN, ProtonVPN, ExpressVPN) to secure internet traffic.
- Run DNS leak tests with services like dnsleaktest.com.
- Use secure cloud storage options such as SpiderOak or Tresorit.

Operational security

- Enforce two-factor authentication (2FA) using tools like Authy or Google Authenticator.
- Staff cybersecurity training and phishing awareness sessions.
- Role-based access control and strict data access policies.

Threat Model: Corresponding with Dissidents

Assets

Threat Model: Corresponding with Dissidents

Assets

- *Confidential Communications:* Secure emails, messages, and correspondence between the researcher and revolutionaries.

Threat Model: Corresponding with Dissidents

Assets

- *Confidential Communications:* Secure emails, messages, and correspondence between the researcher and revolutionaries.
- *Sensitive Research Data:* Reports, documents, and analyses containing politically sensitive or classified information.

Threat Model: Corresponding with Dissidents

Assets

- *Confidential Communications:* Secure emails, messages, and correspondence between the researcher and revolutionaries.
- *Sensitive Research Data:* Reports, documents, and analyses containing politically sensitive or classified information.
- *Reputational Integrity:* The credibility and professional standing of the researcher.

Threat Model: Corresponding with Dissidents

Assets

- *Confidential Communications:* Secure emails, messages, and correspondence between the researcher and revolutionaries.
- *Sensitive Research Data:* Reports, documents, and analyses containing politically sensitive or classified information.
- *Reputational Integrity:* The credibility and professional standing of the researcher.
- *Safety of Correspondents:* The anonymity and security of revolutionary contacts, whose exposure could lead to severe repercussions.

Threat Model: Corresponding with Dissidents

Adversaries

Threat Model: Corresponding with Dissidents

Adversaries

- *Autocratic Regime Security Forces:* Government agencies and intelligence services actively surveilling dissent.

Threat Model: Corresponding with Dissidents

Adversaries

- *Autocratic Regime Security Forces:* Government agencies and intelligence services actively surveilling dissent.
- *Foreign Cyber and Physical Threat Actors:* Entities intent on suppressing political opposition or compromising secure networks.

Threat Model: Corresponding with Dissidents

Adversaries

- *Autocratic Regime Security Forces:* Government agencies and intelligence services actively surveilling dissent.
- *Foreign Cyber and Physical Threat Actors:* Entities intent on suppressing political opposition or compromising secure networks.
- *Malicious Insiders:* Individuals within the communication or data storage chain who may leak sensitive information.

Threat Model: Corresponding with Dissidents

Threat vectors

Threat Model: Corresponding with Dissidents

Threat vectors

- Digital surveillance and interception of communications.

Threat Model: Corresponding with Dissidents

Threat vectors

- Digital surveillance and interception of communications.
- Cyberattacks (phishing, malware, hacking) targeting communication platforms.

Threat Model: Corresponding with Dissidents

Threat vectors

- Digital surveillance and interception of communications.
- Cyberattacks (phishing, malware, hacking) targeting communication platforms.
- Insider compromise, where trusted parties inadvertently or maliciously leak information.

Threat Model: Corresponding with Dissidents

Threat vectors

- Digital surveillance and interception of communications.
- Cyberattacks (phishing, malware, hacking) targeting communication platforms.
- Insider compromise, where trusted parties inadvertently or maliciously leak information.

Vulnerabilities

Threat Model: Corresponding with Dissidents

Threat vectors

- Digital surveillance and interception of communications.
- Cyberattacks (phishing, malware, hacking) targeting communication platforms.
- Insider compromise, where trusted parties inadvertently or maliciously leak information.

Vulnerabilities

- Use of insecure or outdated communication channels/devices.

Threat Model: Corresponding with Dissidents

Threat vectors

- Digital surveillance and interception of communications.
- Cyberattacks (phishing, malware, hacking) targeting communication platforms.
- Insider compromise, where trusted parties inadvertently or maliciously leak information.

Vulnerabilities

- Use of insecure or outdated communication channels/devices.
- Weak operational security (OpSec) practices.

Threat Model: Corresponding with Dissidents

Threat vectors

- Digital surveillance and interception of communications.
- Cyberattacks (phishing, malware, hacking) targeting communication platforms.
- Insider compromise, where trusted parties inadvertently or maliciously leak information.

Vulnerabilities

- Use of insecure or outdated communication channels/devices.
- Weak operational security (OpSec) practices.
- Metadata exposure even when content is encrypted.

Threat Model: Corresponding with Dissidents

Mitigations

Threat Model: Corresponding with Dissidents

Mitigations

- End-to-end encryption for all communications (e.g., Signal).

Threat Model: Corresponding with Dissidents

Mitigations

- End-to-end encryption for all communications (e.g., Signal).
- Use VPNs, Tor, or other anonymizing tools to obscure IP addresses and metadata.

Threat Model: Corresponding with Dissidents

Mitigations

- End-to-end encryption for all communications (e.g., Signal).
- Use VPNs, Tor, or other anonymizing tools to obscure IP addresses and metadata.
- Regularly update software, use secure devices, and compartmentalize sensitive data.

Threat Model: Corresponding with Dissidents

Mitigations

- End-to-end encryption for all communications (e.g., Signal).
- Use VPNs, Tor, or other anonymizing tools to obscure IP addresses and metadata.
- Regularly update software, use secure devices, and compartmentalize sensitive data.
- Enforce data access controls and adopt OpSec training.

Threat Model: Corresponding with Dissidents

Mitigations

Threat Model: Corresponding with Dissidents

Mitigations

- Encourage vulnerable subjects to employ digital countersurveillance techniques like dedicated devices:

Threat Model: Corresponding with Dissidents

Mitigations

- Encourage vulnerable subjects to employ digital countersurveillance techniques like dedicated devices:
  - Use a burner device for sensitive communications (e.g., encrypted messaging, accessing secure email) and a different device for everyday use. If the everyday device is compromised, the sensitive device remains insulated.

Threat Model: Corresponding with Dissidents

Mitigations

- Encourage vulnerable subjects to employ digital countersurveillance techniques like dedicated devices:
  - Use a burner device for sensitive communications (e.g., encrypted messaging, accessing secure email) and a different device for everyday use. If the everyday device is compromised, the sensitive device remains insulated.
- ... or dual-purpose setups:

Threat Model: Corresponding with Dissidents

Mitigations

- Encourage vulnerable subjects to employ digital countersurveillance techniques like dedicated devices:
  - Use a burner device for sensitive communications (e.g., encrypted messaging, accessing secure email) and a different device for everyday use. If the everyday device is compromised, the sensitive device remains insulated.
- ... or dual-purpose setups:
  - Run a secure virtual machine (with hardened security settings) on a host that is used for general tasks. Sensitive operations are performed in a controlled, isolated environment.

Threat Model: Corresponding with Dissidents

Mitigations

- Encourage vulnerable subjects to employ digital countersurveillance techniques like dedicated devices:
  - Use a burner device for sensitive communications (e.g., encrypted messaging, accessing secure email) and a different device for everyday use. If the everyday device is compromised, the sensitive device remains insulated.
- ... or dual-purpose setups:
  - Run a secure virtual machine (with hardened security settings) on a host that is used for general tasks. Sensitive operations are performed in a controlled, isolated environment.
  - Docker containers are ideal burners: cheap and high-quality.

Encryption

Secure Messaging

Secure Messaging

Protecting the anonymity of sources is only sometimes a matter of law but an obvious practical concern if the source may suffer adverse consequences from working with you.

End-to-end encryption

Secure Messaging with Signal

End-to-end encryption

- E.g., “Signal Protocol” ensures that only the communicating devices can read the messages.

Secure Messaging with Signal

End-to-end encryption

- E.g., “Signal Protocol” ensures that only the communicating devices can read the messages.
- Protects against interception and impersonation in the data stream, but of course either device can be compromised.

Secure Messaging with Signal

End-to-end encryption

- E.g., “Signal Protocol” ensures that only the communicating devices can read the messages.
- Protects against interception and impersonation in the data stream, but of course either device can be compromised.

Open-source & audited

Secure Messaging with Signal

End-to-end encryption

- E.g., “Signal Protocol” ensures that only the communicating devices can read the messages.
- Protects against interception and impersonation in the data stream, but of course either device can be compromised.

Open-source & audited

- Code is publicly available and regularly reviewed by security experts.

Secure Messaging with Signal

End-to-end encryption

- E.g., “Signal Protocol” ensures that only the communicating devices can read the messages.
- Protects against interception and impersonation in the data stream, but of course either device can be compromised.

Open-source & audited

- Code is publicly available and regularly reviewed by security experts.

Minimal metadata

Secure Messaging with Signal

End-to-end encryption

- E.g., “Signal Protocol” ensures that only the communicating devices can read the messages.
- Protects against interception and impersonation in the data stream, but of course either device can be compromised.

Open-source & audited

- Code is publicly available and regularly reviewed by security experts.

Minimal metadata

- Designed to retain as little information as possible about your communications.

Secure Messaging with Signal

End-to-end encryption

- E.g., "Signal Protocol" ensures that only the communicating devices can read the messages.
- Protects against interception and impersonation in the data stream, but of course either device can be compromised.

Open-source & audited

- Code is publicly available and regularly reviewed by security experts.

Minimal metadata

- Designed to retain as little information as possible about your communications.
- Even minimal metadata (e.g., "A sent something to B at time t") can be harmful.

Secure Messaging with Signal

End-to-end encryption

- E.g., "Signal Protocol" ensures that only the communicating devices can read the messages.
- Protects against interception and impersonation in the data stream, but of course either device can be compromised.

Open-source & audited

- Code is publicly available and regularly reviewed by security experts.

Minimal metadata

- Designed to retain as little information as possible about your communications.
- Even minimal metadata (e.g., "A sent something to B at time t") can be harmful.

Learn more: Signal Official Website | Signal Security Overview

Evaluating security

Evaluating security

- Look for independent audits and open-source transparency.

Evaluating security

- Look for independent audits and open-source transparency.
- Confirm that the app uses modern encryption standards (e.g., forward secrecy).

Evaluating security

- Look for independent audits and open-source transparency.
- Confirm that the app uses modern encryption standards (e.g., forward secrecy).
- Find reviews by trustworthy independent organizations such as the Electronic Frontier Foundation.

Evaluating security

- Look for independent audits and open-source transparency.
- Confirm that the app uses modern encryption standards (e.g., forward secrecy).
- Find reviews by trustworthy independent organizations such as the Electronic Frontier Foundation.

Additional reading: EFF on Secure Messaging

Secure Traffic

Secure Traffic

Public networks

Secure Traffic

Public networks

- Typically found in places like cafes, airports, hotels, and university campuses.

Secure Traffic

Public networks

- Typically found in places like cafes, airports, hotels, and university campuses.
- Often unencrypted or poorly secured.

Secure Traffic

Public networks

- Typically found in places like cafes, airports, hotels, and university campuses.
- Often unencrypted or poorly secured.
- Vulnerable to eavesdropping and man-in-the-middle attacks.

Secure Traffic

Public networks

- Typically found in places like cafes, airports, hotels, and university campuses.
- Often unencrypted or poorly secured.
- Vulnerable to eavesdropping and man-in-the-middle attacks.

Secured networks

Secure Traffic

Public networks

- Typically found in places like cafes, airports, hotels, and university campuses.
- Often unencrypted or poorly secured.
- Vulnerable to eavesdropping and man-in-the-middle attacks.

Secured networks

- Encrypted and controlled environments (e.g., corporate networks, VPN-secured connections).

Secure Traffic

Public networks

- Typically found in places like cafes, airports, hotels, and university campuses.
- Often unencrypted or poorly secured.
- Vulnerable to eavesdropping and man-in-the-middle attacks.

Secured networks

- Encrypted and controlled environments (e.g., corporate networks, VPN-secured connections).
- Provide stronger protection against external threats.

Secure Traffic

Public networks

- Typically found in places like cafes, airports, hotels, and university campuses.
- Often unencrypted or poorly secured.
- Vulnerable to eavesdropping and man-in-the-middle attacks.

Secured networks

- Encrypted and controlled environments (e.g., corporate networks, VPN-secured connections).
- Provide stronger protection against external threats.

Best practices

Secure Traffic

Public networks

- Typically found in places like cafes, airports, hotels, and university campuses.
- Often unencrypted or poorly secured.
- Vulnerable to eavesdropping and man-in-the-middle attacks.

Secured networks

- Encrypted and controlled environments (e.g., corporate networks, VPN-secured connections).
- Provide stronger protection against external threats.

Best practices

- Use VPNs on public networks.

Secure Traffic

Public networks

- Typically found in places like cafes, airports, hotels, and university campuses.
- Often unencrypted or poorly secured.
- Vulnerable to eavesdropping and man-in-the-middle attacks.

Secured networks

- Encrypted and controlled environments (e.g., corporate networks, VPN-secured connections).
- Provide stronger protection against external threats.

Best practices

- Use VPNs on public networks.
- Avoid accessing sensitive information on untrusted networks.

Secure Traffic

Public networks

- Typically found in places like cafes, airports, hotels, and university campuses.
- Often unencrypted or poorly secured.
- Vulnerable to eavesdropping and man-in-the-middle attacks.

Secured networks

- Encrypted and controlled environments (e.g., corporate networks, VPN-secured connections).
- Provide stronger protection against external threats.

Best practices

- Use VPNs on public networks.
- Avoid accessing sensitive information on untrusted networks.

For more information, see: US-CERT: Protecting Yourself on Public Wi-Fi

Virtual Private Networks (VPNs)

What is a VPN?

Virtual Private Networks (VPNs)

What is a VPN?

- Encrypts your internet traffic and hides your IP address.

Virtual Private Networks (VPNs)

What is a VPN?

- Encrypts your internet traffic and hides your IP address.
- Creates a secure tunnel between your device and a VPN server.

Virtual Private Networks (VPNs)

What is a VPN?

- Encrypts your internet traffic and hides your IP address.
- Creates a secure tunnel between your device and a VPN server.
- You can buy access to a VPN or set up your own.

Virtual Private Networks (VPNs)

What is a VPN?

- Encrypts your internet traffic and hides your IP address.
- Creates a secure tunnel between your device and a VPN server.
- You can buy access to a VPN or set up your own.
- The free ones are not safe.

Virtual Private Networks (VPNs)

What is a VPN?

- Encrypts your internet traffic and hides your IP address.
- Creates a secure tunnel between your device and a VPN server.
- You can buy access to a VPN or set up your own.
- The free ones are not safe.

Evaluating VPN providers

Virtual Private Networks (VPNs)

What is a VPN?

- Encrypts your internet traffic and hides your IP address.
- Creates a secure tunnel between your device and a VPN server.
- You can buy access to a VPN or set up your own.
- The free ones are not safe.

Evaluating VPN providers

- Look for a strict no-logs policy and independent audits.

Virtual Private Networks (VPNs)

What is a VPN?

- Encrypts your internet traffic and hides your IP address.
- Creates a secure tunnel between your device and a VPN server.
- You can buy access to a VPN or set up your own.
- The free ones are not safe.

Evaluating VPN providers

- Look for a strict no-logs policy and independent audits.
- Choose providers in jurisdictions with strong privacy laws.

Virtual Private Networks (VPNs)

What is a VPN?

- Encrypts your internet traffic and hides your IP address.
- Creates a secure tunnel between your device and a VPN server.
- You can buy access to a VPN or set up your own.
- The free ones are not safe.

Evaluating VPN providers

- Look for a strict no-logs policy and independent audits.
- Choose providers in jurisdictions with strong privacy laws.
- Read transparency reports and user reviews.

Virtual Private Networks (VPNs)

What is a VPN?

- Encrypts your internet traffic and hides your IP address.
- Creates a secure tunnel between your device and a VPN server.
- You can buy access to a VPN or set up your own.
- The free ones are not safe.

Evaluating VPN providers

- Look for a strict no-logs policy and independent audits.
- Choose providers in jurisdictions with strong privacy laws.
- Read transparency reports and user reviews.

Further details: Privacy Tools VPN Guide

Confirming Your Traffic is VPN Secured

Check your public IP

Confirming Your Traffic is VPN Secured

Check your public IP

- Use a service like whatismyip.com or ifconfig.me.

Confirming Your Traffic is VPN Secured

Check your public IP

- Use a service like whatismyip.com or ifconfig.me.
- Compare your IP before and after connecting to the VPN.

Confirming Your Traffic is VPN Secured

Check your public IP

- Use a service like whatismyip.com or ifconfig.me.
- Compare your IP before and after connecting to the VPN.

Packet analysis

Confirming Your Traffic is VPN Secured

Check your public IP

- Use a service like whatismyip.com or ifconfig.me.
- Compare your IP before and after connecting to the VPN.

Packet analysis

- Tools like Wireshark can capture packets and confirm that data is encapsulated (encrypted) and not transmitted in plaintext.

Confirming Your Traffic is VPN Secured

Check your public IP

- Use a service like whatismyip.com or ifconfig.me.
- Compare your IP before and after connecting to the VPN.

Packet analysis

- Tools like Wireshark can capture packets and confirm that data is encapsulated (encrypted) and not transmitted in plaintext.

VPN client status:

Confirming Your Traffic is VPN Secured

Check your public IP

- Use a service like whatismyip.com or ifconfig.me.
- Compare your IP before and after connecting to the VPN.

Packet analysis

- Tools like Wireshark can capture packets and confirm that data is encapsulated (encrypted) and not transmitted in plaintext.

VPN client status:

- Check the VPN client's interface and logs to ensure the connection is active and using strong encryption protocols.

Confirming Your Traffic is VPN Secured

Check your public IP

- Use a service like whatismyip.com or ifconfig.me.
- Compare your IP before and after connecting to the VPN.

Packet analysis

- Tools like Wireshark can capture packets and confirm that data is encapsulated (encrypted) and not transmitted in plaintext.

VPN client status:

- Check the VPN client's interface and logs to ensure the connection is active and using strong encryption protocols.

For more details, see the PrivacyTools VPN Guide.

How Tor works

Tor: Enhancing Anonymity

How Tor works

- Routes your internet traffic through multiple relays.

Tor: Enhancing Anonymity

How Tor works

- Routes your internet traffic through multiple relays.
- Masks your originating IP address to provide anonymity.

Tor: Enhancing Anonymity

How Tor works

- Routes your internet traffic through multiple relays.
- Masks your originating IP address to provide anonymity.

Using Tor

Tor: Enhancing Anonymity

How Tor works

- Routes your internet traffic through multiple relays.
- Masks your originating IP address to provide anonymity.

Using Tor

- Download and use the official Tor Browser.

Tor: Enhancing Anonymity

How Tor works

- Routes your internet traffic through multiple relays.
- Masks your originating IP address to provide anonymity.

Using Tor

- Download and use the official Tor Browser.
- Be aware that Tor may slow down your connection and that exit nodes can be vulnerable.

Tor: Enhancing Anonymity

How Tor works

- Routes your internet traffic through multiple relays.
- Masks your originating IP address to provide anonymity.

Using Tor

- Download and use the official Tor Browser.
- Be aware that Tor may slow down your connection and that exit nodes can be vulnerable.

Explore more: Tor Project Official Site

Encryption

- We have previously discussed encryption using SSH keys for asymmetric security.

Encryption

- We have previously discussed encryption using SSH keys for asymmetric security.
- This is useful for setting up persistent connections between two computers, but a bit cumbersome for encrypting data locally or sending encrypted data on a one-off basis.

Encryption

- We have previously discussed encryption using SSH keys for asymmetric security.
- This is useful for setting up persistent connections between two computers, but a bit cumbersome for encrypting data locally or sending encrypted data on a one-off basis.
- Sometimes you just want to encrypt a file with a key and keep the key somewhere safe, or give it to someone else.

Fernet Encryption

- Fernet is a symmetric encryption scheme provided by the Python `cryptography` package.

Fernet Encryption

- Fernet is a symmetric encryption scheme provided by the Python `cryptography` package.
- Designed for ease of use, allowing non-experts to secure sensitive data.

Fernet Encryption

- Fernet is a symmetric encryption scheme provided by the Python `cryptography` package.
- Designed for ease of use, allowing non-experts to secure sensitive data.
- Widely adopted in research and industry for protecting confidential information.

Fernet Encryption

- Fernet is a symmetric encryption scheme provided by the Python `cryptography` package.
- Designed for ease of use, allowing non-experts to secure sensitive data.
- Widely adopted in research and industry for protecting confidential information.
- Helps ensure ethical data handling and compliance with privacy standards.

Fernet Encryption

- Fernet is a symmetric encryption scheme provided by the Python `cryptography` package.
- Designed for ease of use, allowing non-experts to secure sensitive data.
- Widely adopted in research and industry for protecting confidential information.
- Helps ensure ethical data handling and compliance with privacy standards.

For more details, see the Fernet Documentation.

Sender

```python
from cryptography.fernet import Fernet

# Sender: Data to be sent
plaintext = "Confidential: Research subject data."

# Generate symmetric key and encrypt the data
key = Fernet.generate_key()
cipher = Fernet(key)
encrypted_data = cipher.encrypt(plaintext.encode())

# Save encrypted data to file (simulate sending the file)
with open("data.enc", "wb") as f:
    f.write(encrypted_data)

# Display the symmetric key to send securely
print("Send this key to the receiver (on a secure channel):")
print(key.decode())
```

Receiver: Load Encrypted File

```python
from cryptography.fernet import Fernet

# Receiver: Read the encrypted file
with open("data.enc", "rb") as f:
    encrypted_data = f.read()

# Receiver: Use the received key to decrypt
# Paste the key received securely
key = b"PASTE_KEY_HERE"
cipher = Fernet(key)
decrypted_data = cipher.decrypt(encrypted_data)
print("Decrypted data:")
print(decrypted_data.decode())
```

Workflow Explanation and Takeaways

- The sender encrypts the data and saves it to `data.enc`.

Workflow Explanation and Takeaways

- The sender encrypts the data and saves it to `data.enc`.
- The symmetric key is printed—this key must be shared securely with the receiver.

Workflow Explanation and Takeaways

- The sender encrypts the data and saves it to `data.enc`.
- The symmetric key is printed—this key must be shared securely with the receiver.
- The receiver uses the key to decrypt the file, recovering the original data.

Workflow Explanation and Takeaways

- The sender encrypts the data and saves it to `data.enc`.
- The symmetric key is printed—this key must be shared securely with the receiver.
- The receiver uses the key to decrypt the file, recovering the original data.

In practice, always share keys via secure channels (e.g., in-person, via secure messaging, etc.).

General High-Level Advice

Conclusion

- Professional cognitive scientists must at times consider the security and privacy of their digital practices.

Conclusion

- Professional cognitive scientists must at times consider the security and privacy of their digital practices.
  - to protect subjects

Conclusion

- Professional cognitive scientists must at times consider the security and privacy of their digital practices.
  - to protect subjects
  - to protect employers

Conclusion

- Professional cognitive scientists must at times consider the security and privacy of their digital practices.
  - to protect subjects
  - to protect employers
  - to protect themselves

Conclusion

- Professional cognitive scientists must at times consider the security and privacy of their digital practices.
  - to protect subjects
  - to protect employers
  - to protect themselves
- Cybersecurity is a mature field that is partly computer science and math, and partly psychology.

Conclusion

- Professional cognitive scientists must at times consider the security and privacy of their digital practices.
  - to protect subjects
  - to protect employers
  - to protect themselves
- Cybersecurity is a mature field that is partly computer science and math, and partly psychology.
  - there are many tools that enhance security and privacy

Conclusion

- Professional cognitive scientists must at times consider the security and privacy of their digital practices.
  - to protect subjects
  - to protect employers
  - to protect themselves
- Cybersecurity is a mature field that is partly computer science and math, and partly psychology.
  - there are many tools that enhance security and privacy
  - their development is partly technical, but heavily focused on user adoption and retention

Conclusion

- Professional cognitive scientists must at times consider the security and privacy of their digital practices.
  - to protect subjects
  - to protect employers
  - to protect themselves
- Cybersecurity is a mature field that is partly computer science and math, and partly psychology.
  - there are many tools that enhance security and privacy
  - their development is partly technical, but heavily focused on user adoption and retention
  - OpSec is a behavioral concern

Conclusion

- Professional cognitive scientists must at times consider the security and privacy of their digital practices.
  - to protect subjects
  - to protect employers
  - to protect themselves
- Cybersecurity is a mature field that is partly computer science and math, and partly psychology.
  - there are many tools that enhance security and privacy
  - their development is partly technical, but heavily focused on user adoption and retention
  - OpSec is a behavioral concern
  - knowing which tools are secure is a matter of trust (of the vendor, or the reviewer)

Conclusion

If online privacy is important to you:

Know nothing is 100% secure

Conclusion

If online privacy is important to you:

Know nothing is 100% secure

- Privacy risk cannot be eliminated, only mitigated

Conclusion

If online privacy is important to you:

Know nothing is 100% secure

- Privacy risk cannot be eliminated, only mitigated
- Anything stored or transmitted electronically may be vulnerable

Conclusion

If online privacy is important to you:

Know nothing is 100% secure

- Privacy risk cannot be eliminated, only mitigated
- Anything stored or transmitted electronically may be vulnerable
- If it really needs to be secret, you should not write it down

Conclusion

If online privacy is important to you:

Know nothing is 100% secure

- Privacy risk cannot be eliminated, only mitigated
- Anything stored or transmitted electronically may be vulnerable
- If it really needs to be secret, you should not write it down

Layer your defenses

Conclusion

If online privacy is important to you:

Know nothing is 100% secure

- Privacy risk cannot be eliminated, only mitigated
- Anything stored or transmitted electronically may be vulnerable
- If it really needs to be secret, you should not write it down

Layer your defenses

- Use multiple security measures (encryption, secure messaging, VPNs, Tor, good OpSec, constant vigilance) to mitigate risk

Conclusion

If online privacy is important to you:

Know nothing is 100% secure

- Privacy risk cannot be eliminated, only mitigated
- Anything stored or transmitted electronically may be vulnerable
- If it really needs to be secret, you should not write it down

Layer your defenses

- Use multiple security measures (encryption, secure messaging, VPNs, Tor, good OpSec, constant vigilance) to mitigate risk
- Do not rely on security through obscurity

Conclusion

If online privacy is important to you:

Know nothing is 100% secure

- Privacy risk cannot be eliminated, only mitigated
- Anything stored or transmitted electronically may be vulnerable
- If it really needs to be secret, you should not write it down

Layer your defenses

- Use multiple security measures (encryption, secure messaging, VPNs, Tor, good OpSec, constant vigilance) to mitigate risk
- Do not rely on security through obscurity
- Kerkhoff's Principle: "Design your system assuming that your opponents know it in detail"

Conclusion

If online privacy is important to you:

Know nothing is 100% secure

- Privacy risk cannot be eliminated, only mitigated
- Anything stored or transmitted electronically may be vulnerable
- If it really needs to be secret, you should not write it down

Layer your defenses

- Use multiple security measures (encryption, secure messaging, VPNs, Tor, good OpSec, constant vigilance) to mitigate risk
- Do not rely on security through obscurity
- Kerkhoff's Principle: "Design your system assuming that your opponents know it in detail"

Keep software up to date

Conclusion

If online privacy is important to you:

Know nothing is 100% secure

- Privacy risk cannot be eliminated, only mitigated
- Anything stored or transmitted electronically may be vulnerable
- If it really needs to be secret, you should not write it down

Layer your defenses

- Use multiple security measures (encryption, secure messaging, VPNs, Tor, good OpSec, constant vigilance) to mitigate risk
- Do not rely on security through obscurity
- Kerkhoff's Principle: "Design your system assuming that your opponents know it in detail"

Keep software up to date

- Regularly update your operating systems and applications to patch known vulnerabilities.

Conclusion

Compartmentalize sensitive data

Conclusion

Compartmentalize sensitive data

- Separate sensitive information from routine work files.

Conclusion

Compartmentalize sensitive data

- Separate sensitive information from routine work files.

Secure your communications and online privacy

Conclusion

Compartmentalize sensitive data

- Separate sensitive information from routine work files.

Secure your communications and online privacy

- Use Signal for encrypted messaging.

Conclusion

Compartmentalize sensitive data

- Separate sensitive information from routine work files.

Secure your communications and online privacy

- Use Signal for encrypted messaging.
- Leverage VPNs and Tor for secure and anonymous browsing.

Conclusion

Compartmentalize sensitive data

- Separate sensitive information from routine work files.

Secure your communications and online privacy

- Use Signal for encrypted messaging.
- Leverage VPNs and Tor for secure and anonymous browsing.

Protect your files

Conclusion

Compartmentalize sensitive data

- Separate sensitive information from routine work files.

Secure your communications and online privacy

- Use Signal for encrypted messaging.
- Leverage VPNs and Tor for secure and anonymous browsing.

Protect your files

- Use simple, reproducible encryption methods (e.g., in Python).

Conclusion

Compartmentalize sensitive data

- Separate sensitive information from routine work files.

Secure your communications and online privacy

- Use Signal for encrypted messaging.
- Leverage VPNs and Tor for secure and anonymous browsing.

Protect your files

- Use simple, reproducible encryption methods (e.g., in Python).
- Encrypt entire drives (e.g., with VeraCrypt).

Conclusion

Compartmentalize sensitive data

- Separate sensitive information from routine work files.

Secure your communications and online privacy

- Use Signal for encrypted messaging.
- Leverage VPNs and Tor for secure and anonymous browsing.

Protect your files

- Use simple, reproducible encryption methods (e.g., in Python).
- Encrypt entire drives (e.g., with VeraCrypt).
- Do not invent your own, you will lose every time.

Conclusion

Compartmentalize sensitive data

- Separate sensitive information from routine work files.

Secure your communications and online privacy

- Use Signal for encrypted messaging.
- Leverage VPNs and Tor for secure and anonymous browsing.

Protect your files

- Use simple, reproducible encryption methods (e.g., in Python).
- Encrypt entire drives (e.g., with VeraCrypt).
- Do not invent your own, you will lose every time.

Cut luxuries

Conclusion

Compartmentalize sensitive data

- Separate sensitive information from routine work files.

Secure your communications and online privacy

- Use Signal for encrypted messaging.
- Leverage VPNs and Tor for secure and anonymous browsing.

Protect your files

- Use simple, reproducible encryption methods (e.g., in Python).
- Encrypt entire drives (e.g., with VeraCrypt).
- Do not invent your own, you will lose every time.

Cut luxuries

- Do your data need to be transmitted at all? (Not a lot beats an air gapped computer for network safety.)

Conclusion

Compartmentalize sensitive data

- Separate sensitive information from routine work files.

Secure your communications and online privacy

- Use Signal for encrypted messaging.
- Leverage VPNs and Tor for secure and anonymous browsing.

Protect your files

- Use simple, reproducible encryption methods (e.g., in Python).
- Encrypt entire drives (e.g., with VeraCrypt).
- Do not invent your own, you will lose every time.

Cut luxuries

- Do your data need to be transmitted at all? (Not a lot beats an air gapped computer for network safety.)
- Keep a small team to better control access.

Conclusion

Compartmentalize sensitive data

- Separate sensitive information from routine work files.

Secure your communications and online privacy

- Use Signal for encrypted messaging.
- Leverage VPNs and Tor for secure and anonymous browsing.

Protect your files

- Use simple, reproducible encryption methods (e.g., in Python).
- Encrypt entire drives (e.g., with VeraCrypt).
- Do not invent your own, you will lose every time.

Cut luxuries

- Do your data need to be transmitted at all? (Not a lot beats an air gapped computer for network safety.)
- Keep a small team to better control access.

Additional tips: EFF Security Self-Defense Guide

Protecting Research Integrity with Secure Data and Communication Practices