

Security Tips & Best Practices

for
Individuals &
Organizations



Congratulations!

You've taken the first step toward protecting yourself and your organization from cyber threats.

By picking up this booklet, you're already ahead of the curve, investing in the knowledge and tools that are essential to staying secure online.

Inside, you'll find straightforward, practical security tips to help strengthen your defenses against common cyber threats. We'll cover everything from protecting personal information to key business practices you can implement with your team.

This information is here to help you and your organization recognize and respond to cyber risks, giving you a solid foundation to tackle whatever digital challenges come your way.

Let's make every step forward a secure one. You won't regret it!



About NetGain Technologies

Cybersecurity is a critical challenge, impacting many aspects of life and business. As an award-winning Managed Security Service Provider (MSSP), NetGain Technologies empowers organizations to confidently navigate cyber threats. Our managed IT and cybersecurity solutions keep your infrastructure secure, responsive, and always operational, so you can focus on growing your business. With four decades of experience supporting local business and a strong regional presence, NetGain has helped thousands of companies build cyber resilience and achieve their business goals.

**For more information about NetGain Technologies, visit
www.NetGainIT.com**

For Individuals

- ☐  **Email Account Management**
Do you have old email accounts on social platforms? When was the last time you accessed it?
- ☐  **Confidential/Sensitive Data**
Have you stored confidential/sensitive documents in your emails (sent folder, archives)?
- ☐  **Password Management**
People commonly re-use good passwords. This can be a major cause of data breaches.
- ☐  **Security Questionnaires**
Most people have security question answers for sale on the dark web, through prior breaches of the account host. Are your answers to questions potentially listed on your social media accounts or found online?
- ☐  **Secure Your Finances**
Most people don't freeze their credit. When your ID is stolen, debt can be incurred and credit score ruined.
- ☐  **Travel Safety**
Are you using a VPN when traveling? Are you detailing your whereabouts in your out-of-office message?
- ☐  **Online Threats**
Are you verifying web vendors before you make online purchases?
- ☐  **Home Safety**
Are you leaving devices in your vehicle? Are you using any sort of home security/monitoring devices?

For Organizations

- ☐  **vCSO Strategic Consulting**
Do you have CISSP-certified security experts on staff or engaged on an ongoing basis?
- ☐  **Security Awareness Training**
Does your business practice security awareness training? How strong is your company's security culture?
- ☐  **Security Assessments**
Do you conduct internal and external penetration tests on (at least) a quarterly basis?
- ☐  **Incident Response**
Do you have an incident response team with tested IRPs? Do you practice tabletop exercises to ensure readiness?
- ☐  **Email Protection**
Does your email protection include spam filtering, content filtering, and advanced threat detection?
- ☐  **Endpoint & Server Protection**
Antivirus is dead. Are you equipped with next-generation endpoint detection and response?
- ☐  **Advanced Threat Protection**
Do you have malware protection with built-in forensics capabilities?
- ☐  **Risk Assessment**
Have you conducted a risk assessment within the last 12-18 months?
- ☐  **SOC-as-a-Service**
Are you using AI to detect security risks across event logs, syslog's, servers, and devices?

REMOTE WORK BEST PRACTICES

01 DON'T DELAY SOFTWARE UPDATES

Don't delay software updates, as they often contain critical security patches to protect against vulnerabilities. Keeping devices and applications up to date ensures they can defend against the latest cyber threats and helps maintain system performance and reliability.

02 DON'T TURN OFF THE VPN

Use only company-provided devices for Virtual Private Network (VPN) connections and keep all systems updated with the latest patches. Enable Multi-Factor Authentication (MFA) for added security, and stay vigilant about home network security to prevent malware from spreading to corporate networks.

03 WATCH OUT FOR PHISHING SCAMS

Stay alert for phishing scams when working remotely by verifying email senders and avoiding suspicious links or attachments. Double-check email addresses, confirm urgent requests through another method, and encrypt sensitive information before sending it outside the company.

04 PUMP UP THE PASSWORDS

Use strong, unique passwords for all accounts, and update them regularly to enhance security. Avoid using easily guessed information, like birthdays, and consider using a password manager to generate and store complex passwords securely.

05 KEEP YOUR DEVICES SEPARATE

Avoid mixing personal and work devices to reduce security risks. Use company-provided devices only for work tasks to protect sensitive data and prevent personal device vulnerabilities from impacting the corporate network.

06 USE MULTI-FACTOR AUTHENTICATION (MFA)

Always enable MFA for an added layer of security. MFA requires additional verification, such as a code from an app or a fingerprint, making it much harder for attackers to access your accounts. It's a simple and effective way to protect sensitive data.



EMAIL SECURITY

BEST PRACTICES



Beware of Phishing

Look out for phishing email warning signs like grammatical errors, unfamiliar email addresses, urgent requests, or demands for money or login credentials. If you spot any of these, report the email and avoid the scam.



Turn on Spam Filters

Email providers use spam filters to automatically redirect suspicious or irrelevant messages to a separate folder, where you can review or delete them.



Enable Multi-Factor Authentication (MFA)

MFA protects against many email attacks by requiring additional identity verification, which makes it nearly impossible for hackers to replicate your identity.

IDENTITY THREAT DETECTION & RESPONSE

Identity Threat Detection & Response (ITDR) acts as a dedicated security system for your email. It combines advanced technology with human expertise to monitor for suspicious activity, such as unusual logins or hidden email rules. If a threat is detected, ITDR quickly stops the attack, resolves the issue, and strengthens your defenses to prevent future incidents.



Create Strong Passwords

Passwords are your first line of defense against hackers, especially for email accounts. Strong, reliable passwords protect from attacks that target weak or exposed passwords.

BUSINESS EMAIL COMPROMISE

92% of Cyberattacks are Initiated Through Email

Business Email Compromise (BEC) is a type of cybercrime where the scammer uses email to trick someone into sending money or divulging company information. BEC is one of the most financially draining online crimes and is often referred to as The Billion Dollar Scam. Protecting your business against BEC through Managed Identity Threat Detection & Response (Managed ITDR) is vital.



Download Antivirus Software

Antivirus software is a powerful tool for combating email threats like spear phishing and ransomware. Its advanced malware detection and removal features alert you to potential threats and eliminate them once confirmed.



Never Download Attachments from Suspicious Messages

Cybercriminals often use phishing emails with malicious attachments to spread malware. Be cautious with email files, especially on personal and work accounts. If you don't recognize the sender, delete the message.



01 Emphasizing Password Length Over Complexity

NIST now advises that longer passwords are more secure than complex ones. Users should create passwords with a minimum of 8 characters, with a best practice of at least 15 characters. Systems should allow passwords up to 64 characters and accept all printable ASCII and Unicode characters.



02 Eliminating Mandatory Password Changes

Routine password changes are no longer recommended unless there's evidence of a security breach. Frequent changes can lead to weaker passwords, as users may opt for simpler, more predictable choices.

03 Avoiding Password Composition Rules

NIST advises against enforcing complexity requirements, such as mandating the use of uppercase letters, numbers, or special characters. These rules often result in predictable patterns that can be exploited.

PASSWORD BEST PRACTICES

04 Implementing Password Blocklists

Organizations should maintain blocklists to prevent the use of commonly compromised or easily guessable passwords, enhancing overall security.

05 Encouraging the Use of Password Managers

To help users manage complex and lengthy passwords, NIST recommends the use of password managers, which can securely store and generate strong passwords.



Keeping Children Safe Online



The Digital Age & Our Children

In a world where technology is second nature to children, ensuring their safety online is more important than ever. From social media platforms to gaming apps, children are exposed to risks such as cyberbullying, inappropriate content, and online predators. However, with the right practices, you can create a safe and secure digital environment.

Be a Role Model

Children learn by example. Show them healthy online habits by being cautious with what you share and maintaining digital privacy.

Set Up Parental Controls

Parental controls are your first line of defense. Most devices and apps offer settings to restrict access to inappropriate content and monitor usage. Use tools like Google Family Link or built-in parental settings to customize the level of access your child has.

Set Screen Time Limits

Establish clear boundaries for screen time to ensure kids balance their online and offline activities. Tools like Apple Screen Time or Android's Digital Wellbeing can help manage and monitor usage effectively.

Educate About Cybersecurity

Teach your children the basics about staying safe online:

- Passwords: Help them create strong passwords and stress the importance of not sharing with others.
- Stranger Danger: Explain why they should never share personal information with strangers, even in online games.
- Phishing Awareness: Show them how to recognize suspicious email, messages, and links.



Encourage Open Communication

Build a relationship of trust where your children feel comfortable sharing their online experiences. Ask questions like:

- "What websites or apps do you enjoy the most?"
- "Have you ever seen anything online that made you feel uncomfortable?"

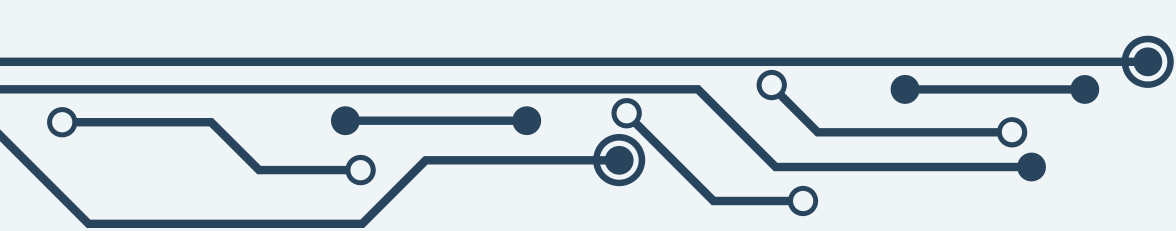
Regularly Review Privacy Settings

Regularly review privacy settings to keep profiles private and limit access to trusted friends and family.

KEY TAKEAWAYS:

- Use parental controls to restrict access to unsafe content.
- Teach basic cybersecurity skills to protect personal information.
- Foster open communication to ensure your child feels safe reporting concerns.
- Maintain balance with screen time limits and offline activities.





Phone Safety Tips

Use a Six-Digit Passcode

Start with a strong six-digit passcode to make it harder for unauthorized users to access your phone.

Enable Find My Phone/Device

These built-in tracking tools help locate a lost or stolen device. With activation lock, it also prevents others from using your phone without permission.

Disable Location Sharing for Photos

Photos often store location by default. To turn this off, go to Settings and Location Services for your Camera app and select "Never." This ensures your photos don't share geotags.

Use Sign in with Apple

When creating accounts, opt for Sign in with Apple. This masks your email and limits how much personal information is shared with third parties.

Turn off Wi-Fi & Bluetooth Auto-Connect

Avoid connecting to unknown networks by disabling auto-connect under Settings within your wi-fi preferences for unfamiliar devices.

Leverage Browser Privacy Features

Enable Prevent Cross-Site Tracking and Hide IP Address under Settings to block advertisers and protect your online identity.

Use Touch ID or Face ID

Protect individual apps with biometric security for added privacy.

Install a VPN

Use a VPN to protect data when connected to unfamiliar networks.

Monitor Your Privacy Settings

Regularly review app permissions under Settings and revoke any unnecessary access.

Turn on USB Restricted Mode

Prevent hackers from using your USB charging port to install malware.

Disable Lock Screen Options

Minimize lock screen widgets to reduce the risk of exposing personal information at a glance.

Install Updates Promptly

Keep your phone up to date to ensure it has the latest security patches.

Avoid Using Third-Party Apps

Stick to trusted apps from the App Store to reduce security risks.

Limit Ad Tracking

Under Settings, toggle off "Allow Apps to Request to Track" to prevent data collection across apps and websites.



Victim of Credit Card Fraud?



01 DETERMINE IF YOU'RE A VICTIM

To detect and address credit card fraud, regularly check your credit report for unauthorized accounts, sign up for credit monitoring services, and review all financial accounts for suspicious activity. If fraud is detected, organize related documentation, change your account passwords, and secure your information to prevent further breaches.

02 CALL THE CREDIT CARD'S FRAUD DEPARTMENT

Contact your credit card's fraud department to report unauthorized accounts, request account closures, and have fraudulent charges removed. Keep a log of all communications. Remember, fraud departments are there to assist victims, so follow their guidance and retain information for follow-up.

03 CONTACT THE 3 NATIONAL CREDIT BUREAUS

Place a security freeze on your credit with all three bureaus (Equifax, Experian, and TransUnion) to block unauthorized accounts. Unfreeze it temporarily if needed for specific transactions. Add a fraud alert to your credit report to require lenders to verify your identity before approving credit; this alert lasts one year and can be renewed, with extended alerts available for identity theft victims.

04 GET THE GOVERNMENT INVOLVED

File an Identity Theft Report with the Federal Trade Commission at [IdentityTheft.gov](https://www.ftc.gov/identity-theft) to document the fraud and receive a recovery plan, keeping a copy for creditors who may require it. File a police report with your local authorities, as it may be needed by credit card issuers to remove fraudulent charges and verify your identity.

05 CONTACT ISSUERS AND CREDIT BUREAUS, AGAIN

Persistently request removal of fraudulent charges with your FTC Identity Theft Report and secure written confirmation of account closures. Submit a written request to credit bureaus to block fraudulent debts from your credit report and prevent them from going to collections.

06 DON'T PAY ANY FRAUDULENT DEBT

Avoid paying fraudulent debt, as it may be seen as accepting responsibility, making it harder to dispute later. If issuers are uncooperative, seek help from an attorney, Legal Aid, or the Identity Theft Resource Center for free assistance.



FREEZE YOUR CREDIT

HOW TO GUIDE

What is a Credit Freeze?

A credit freeze blocks access to your credit report, protecting against fraud. You'll need your Social Security number, date of birth, address, and possibly ID verification. A freeze stays until you lift it and can be temporarily unfrozen.

How to Freeze Your Credit

Freezing your credit can be done online, by phone, or by mail. Online and phone requests are processed more quickly, while mailed requests take longer.

Why Freeze Your Credit?

A credit freeze is an effective way to prevent identity theft. It stops scammers from opening accounts since you block access to your credit report.

Cons of Freezing Your Credit

A credit freeze blocks new account fraud but doesn't stop unauthorized charges on existing accounts. You'll need to lift it to apply for credit, and it may complicate creating accounts like mySocialSecurity.

Unfreezing Your Credit

You can unfreeze your credit online, by phone, or by mail. Online and phone requests are processed more quickly, while mailed requests take longer.

Who Can Access Frozen Credit?

Even with a credit freeze, you can access your own reports. Current creditors, debt collectors, marketers, and certain government agencies can still view them.

Credit Freeze vs. Credit Lock

A credit freeze is free and federally mandated and offers strong protection. A credit lock is a paid service with fewer legal protections, and is often included in subscription packages.

TRAVELING? CYBER SAFETY

Traveling comes with unique cyber risks. Protect your devices, data, and finances with these simple tips before, during, and after your trip.



BEFORE YOU LEAVE

Bring only essential devices secured with strong passwords or biometric locks. Carry minimal payment cards with fraud protection and enable alerts. Update all software and operating systems.



AT THE AIRPORT

Avoid public Wi-Fi and USB charging stations; use your own hotspot and personal charger to prevent potential malware attacks.



AT YOUR DESTINATION

Use a hotspot or VPN for secure internet access and avoid public Wi-Fi. Disable automatic connections to unknown wireless or bluetooth networks. Avoid public computers and keep a close eye on your devices.



WHEN TRAVELING INTERNATIONALLY

Limit sensitive transactions and use debit cards only at secure ATMs. Opt for credit card chip readers instead of swiping. In high-risk countries, use a disposable phone to safeguard your data.



WHEN YOU RETURN

Review your device and account security, especially if working remotely, to ensure no breaches occurred during your trip.



Personal Protection Resources



Personal Security Resources

- **Check Links** for Malware/Phish etc: [HERE](#)
- **Delete Your Private Data** from the Internet/Data Brokers: <https://get.optery.com/LiveTraining>
- Consider **DELETE ME** (20% Code to Remove Data Brokers) [HERE](#)
- **What Breaches Have Effected You?** <https://haveibeenpwned.com/>
- **Scan the DARK WEB (safely) (Is Your Data for Sale?)**
Personal Scan: <https://www.keepersecurity.com/free-data-breach-scan.html>
Work Email Scan: <https://www.keepersecurity.com/data-breach-scan-for-business.html>

Online Shopping and Vendor Safety

- Verify Web Vendors Before You Buy: <https://www.getsafeonline.org/checkawebsite/>
- Website Scam Checker: <https://www.scamadviser.com>
- Use Privacy Cards When Shopping Online: <https://privacy.com>

Password and Link Security

- Test Your Password Strength: <https://www.security.org/how-secure-is-my-password/>
- Check if a Link is a PHISH: <https://check.getsafeonline.org>

Delete Your Private Data Online: Personal Privacy Help

- **Delete Your Private Data (Free & Low cost) from the Internet, Data Brokers, Search Engines & More:**
- **DELETE ME** (20% Code to Remove Data Brokers) [HERE](#) or try Optery <https://get.optery.com/LiveTraining>
- **Scan Your Online Private Data:** <https://incogni.com/digital-footprint-checker>
- **Scan Websites** for Safety: & Malware [HERE](#)

FREEZE Your Credit Today (and Children's too) on All 3 Credit Agencies

Guides give step-by-step (plus how to freeze minors credit by mail)

Equifax Guide: www.nerdwallet.com/article/finance/equifax-credit-freeze

Experian Guide: www.nerdwallet.com/article/finance/experian-credit-freeze

TransUnion Guide: www.nerdwallet.com/article/finance/transunion-credit-freeze

Once Guides are reviewed, Freeze here:

Equifax <https://www.equifax.com/personal/credit-report-services/credit-freeze/>

Experian <https://www.experian.com/help/credit-freeze/>

TransUnion <https://www.transunion.com/credit-freeze>

Lifestyle and Safety Tips

Need Help with Gaming Online Addiction?

<https://www.getsafeonline.org/personal/articles/online-gaming/>

Online Dating Safety:

<https://www.getsafeonline.org/personal/articles/online-dating/>

Health and Legal Concerns

- Fix Online Health Records if Inaccurate: <https://www.hhs.gov/hipaa/for-individuals/medical-records/index.html>

Child Safety and Sextortion

- Remove Explicit Online Photos: <https://www.youtube.com/watch?v=RoilZ7AHb1U&t=215s>
- How to Report Sextortion: <https://report.cybertip.org>

Password Managers

Some free some low cost and some offer VPN as well.

Samples: NORD, KEEPER, IRONVEST, PROTON



Essential Security

for Organizations

