isp.net Cyber Safety Guide

Protecting Families and Businesses Online

Online threats are everywhere — and they're growing. According to the SBA, 43% of cyberattacks target small businesses, yet only 14% are prepared. Families are at risk too, with scams popping up through texts, emails, voicemails, and even social media.

But what are scammers really after? Most cybercriminals have one goal: **money.** They want your passwords, bank details, Social Security numbers, or anything they can sell on the dark web. Some will try to hijack your email or social media accounts to trick your friends and customers. Others go after businesses to steal customer data or shut down systems until a ransom is paid.

At isp.net, our role is about more than providing internet. We're here to keep our community safe, informed, and connected. This guide breaks cybersecurity into simple steps anyone can take — no IT background required.

1. How to Spot and Avoid Phishing Emails and Texts

Phishing happens when scammers pretend to be someone you trust — a bank, delivery service, or even a government office — to trick you into clicking a link or sharing info.

Red flags to watch for:

- Messages that create panic: *"Your account will be shut down today!"*
- Misspelled words, odd email addresses, or strange formatting
- Links that don't match the real site (hover to check before clicking)
- **Suspicious sender addresses** — legit businesses use clear, professional email domains (like *@company.com*). If the "from" address looks random or mismatched, it's likely a scam.

Stay safe:

- Don't click links or open attachments from unknown senders
- Always double-check the sender's email address before replying or clicking
- When in doubt, go directly to the official website or call the company
- Report suspicious messages to your email provider or carrier

Once you know how to spot phishing scams, the next step is making sure even if your credentials are exposed, attackers can't easily access your accounts. That starts with strong passwords and multi-factor authentication.

2. Strong Passwords and Multi-Factor Authentication (MFA)

A password alone isn't enough. Hackers guess, steal, or buy them from leaks every day. That's why MFA adds an extra lock — like a code texted to your phone or a fingerprint scan.

What is MFA? Multi-Factor Authentication (MFA) is an added security step that requires two or more ways to verify your identity—for example, a password **plus** a one-time code sent to your phone, or a fingerprint scan. Even if a hacker gets your password, they still can't log in without the second factor.

Smart practices:

- Use at least 12 characters with numbers, letters, and symbols
- Skip personal details like birthdays or pet names
- Use a password manager to stay organized
- Turn on MFA for email, banking, and shopping accounts

Pro Tip:

Think of MFA like a seatbelt — quick, simple, and lifesaving when it matters. Understanding how criminals exploit sensitive information can help you stay a step ahead.

3. Protecting Personal and Financial Information

Your personal data—like Social Security numbers, credit card details, or even your date of birth—is incredibly valuable. Criminals can use it for fraud, identity theft, or to sell on the dark web. Treat your data like cash—it's worth protecting.

Types of fraud you may face:

- **Identity theft**: Opening bank accounts or credit cards in your name
- **Financial fraud**: Unauthorized charges, drained accounts, or loan scams
- **Account takeovers**: Hackers hijack your email or social media for scams
- **Medical fraud**: Using your health insurance for fake claims
- **Tax fraud**: Filing false tax returns using your stolen identity

How your data gets misused:

- A stolen email + password might let hackers access your online banking
- Oversharing details on social media helps scammers guess security answers
- Leaked credit card info can be used for purchases worldwide

Best practices to protect yourself:

- Shop only on secure sites (**https://** + padlock symbol)
- Limit what you share online — avoid posting full birthdays, addresses, or phone numbers
- Don't enter sensitive info on public Wi-Fi unless using a VPN
- Check bank and credit accounts regularly for suspicious activity
- Keep all devices updated with the latest security patches.

Protecting your data is just one piece of the puzzle. Businesses hold even more sensitive customer information — and we'll look next at how they can protect it affordably.

4. Affordable Cybersecurity for Small Businesses

Many small businesses think cyberattacks only happen to large corporations, but that misconception makes them vulnerable. In reality, attackers know smaller organizations often lack strong defenses, making them easy targets.

Practical steps:

- Use **cloud-based email and storage** with built-in security (Google Workspace, Microsoft 365)
- Train employees to recognize phishing attempts and avoid risky behavior
- Set up automatic **data backups** both locally and in the cloud
- Restrict employee access so only authorized staff handle sensitive data
- Install and update antivirus software and enable firewalls
- Write a simple **cybersecurity policy** to guide staff actions

Even with strong precautions, no system is immune. That's why it's essential to know what to do if a cyber incident does occur.

5. Protecting Company Servers with ColoNet

For businesses that rely on servers, data centers, or networking gear, isp.net offers **ColoNet** — secure, scalable, and locally supported colocation built for serious businesses in Southern Nevada.

- **Secure, Climate-Controlled Rack Space**
  Ideal for servers, storage, or networking gear—with unmatched physical and digital security.

- **Fully Redundant Networking**
  BGP-optimized, carrier-blended bandwidth up to 100Gb for maximum uptime and performance.

- **A Local Partner You Can Trust**
  Colocation isn't just about space and power—it's about trust, uptime, and having a partner who stands behind their promise. With isp.net, businesses know their systems are protected by a local team that values relationships as much as reliability.

ColoNet gives businesses the confidence that their critical systems are protected, backed by local experts who know them by name—not ticket number.

6. Reporting and Recovering from Cyber Incidents

Cyber incidents can be overwhelming, but quick action minimizes the damage. Whether it's a hacked email, stolen bank details, or ransomware, responding calmly and swiftly can protect your finances, reputation, and peace of mind. Remember: the faster you act, the harder it is for criminals to profit from the attack.

What to do first:

1. **Disconnect** from the internet to stop further damage
2. **Change passwords** immediately, starting with email and banking accounts
3. **Enable MFA** if not already on
4. **Report scams** to:
    - **FTC (U.S.):** reportfraud.ftc.gov
    - **IC3 (FBI):** ic3.gov (for online crime)
    - Your **bank/credit card company** for financial fraud
    - Your **local police** if identity theft occurs

Recovery steps:

- Run antivirus scans to remove malware
- Restore files from clean backups if corrupted
- Seek professional IT help if your business operations are disrupted

Building Cyber Confidence

Knowing how to respond and recover is the final step in building cyber confidence. With the right habits, tools, and awareness, families and businesses can take control of their online safety.

At isp.net, cybersecurity is about preparation. From spotting phishing scams to strengthening accounts with MFA, from protecting personal data to securing business systems with ColoNet, we're here to make every step simpler and stronger.

When people and businesses take small, consistent steps toward cybersecurity, the entire community benefits. Together, we can create a safer, smarter, and more connected online future.