🛡️ 2025 Seasonal Cyber Threat Survival Guide

🚨 Cybersecurity threats **increase significantly** from November through April due to seasonal sales and tax-related activities. This guide provides practical steps to protect your personal and professional information.

⚠️ Modern Threats & Defense Strategies

This guide details the threat type, how the attacks work, and the essential defense rules.

🗄️ Threat Type	Explanation (The Rule)	⚙️ How It Works (The Mechanism)
📧 **Email Phishing**	**Always verify the sender** and **avoid clicking** on suspicious attachments or links.	Spoofs legitimate domains and uses **urgent language** to bypass rational thinking. Often includes malicious links/attachments or redirects to fake, identical login pages to steal credentials.
🛑 **Scam Redirect Pages**	These pages aim to **scare you** into calling the attacker or paying for fake services.	Uses **JavaScript/pop-up overlays** to block navigation and mimic system alerts ("Your computer is infected!"). Includes audio warnings and urgent instructions to call a scammer posing as tech support.
👥 **Social Hacking**	Exploits **trust and human error** rather than technical flaws. Attackers impersonate colleagues or gather personal details to create convincing scenarios.	Relies on **psychological manipulation**: • **Pretexting:** Fabricated scenarios to get info. • **Baiting:** Offering something enticing to lure the victim. • **Tailgating:** Following authorized personnel into restricted areas.
📞 **Phone Call Phishing (Vishing)**	**Never share sensitive information** unless you **initiate the call** to a verified number.	Uses **Caller ID spoofing** and scripts to impersonate trusted entities (banks, government) and create **urgency** to extract personal or financial data.
🤖 **AI-Driven Scams**	Be **cautious of urgent requests**. Always **verify identities** through official, established channels.	Uses machine learning to **mimic voices** (deepfakes) and generate realistic conversations. Deepfake audio can sound identical to someone you know, making verification paramount.

✅ Your Practical Protection Checklist

- ☐ **Verify Identity:** Use a different, trusted channel (e.g., call them back on a known, official number) to confirm urgent requests.
- ☐ **Check URLs:** Hover over links (don't click!) to check the true destination URL for any spoofed domains.
- ☐ **Don't Panic:** Scammers use urgency to make you act without thinking. Take a moment to analyze the situation.
- ☐ **Educate Yourself:** Share this knowledge! Social hacking relies on human vulnerability.