# Demystifying Cyber Threats: Protecting Against Phishing, Smishing, and Vishing

In today's technologically advanced world, our reliance on digital communication and online services has grown exponentially. Increased connectivity provides cybercriminals the opportunity to exploit a greater number of platforms and users. Hackers have also become more adept at exploiting vulnerabilities and tricking unsuspecting individuals into revealing sensitive information like personal health information (PHI). Three common cyber threats that pose a significant risk to individuals and health care organizations are phishing, smishing, and vishing. This bulletin considers these types of cyber attacks, their modus operandi, and suggestions to protect yourself from falling victim to these tactics.

## 1. Phishing: The Elusive Art of Baiting

Phishing is one of the most prevalent cyber threats, where attackers use **email messages** to impersonate reputable entities to obtain sensitive information, such as usernames, passwords, credit card details, PHI, or other personal data. Phishing attacks occur through fraudulent emails, which mimic legitimate communications from third parties such as family, friends, health-care organizations, banks or other trusted sources. These emails often contain urgent or alarming messages, pushing recipients to act hastily without verifying the authenticity of the sender.

How Phishing Works:

- Cyber criminals create deceptive emails or messages that seem genuine, complete with logos and formatting to mislead recipients.
- The messages often contain a call to action, such as clicking a link to update account information or confirming login credentials on a fake website.
- Once the victim falls for the bait and provides their data, the attackers gain unauthorized access to sensitive accounts or information.

## 2. Smishing: The Menace of Text Message Scams

Smishing, a blend of "SMS" and "phishing," is a cyber threat that uses **text messages** to deceive recipients. These messages typically contain a sense of urgency or excitement, encouraging users to click malicious links or respond with personal information. Smishing attacks are particularly dangerous because mobile users often assume that text messages are more trustworthy than emails.

How Smishing Works:

- Cyber criminals send text messages that appear to be from legitimate sources, such as banks, retailers, health-care organizations, or government agencies.
- The messages often contain alarming news, enticing offers, or fake prize notifications, prompting recipients to take immediate action.
- Clicking on the embedded links may lead victims to malicious websites designed to steal personal information or install malware on their devices.

### 3. Vishing: The Silver-Tongued Voice Scam

Vishing, short for "voice phishing," is a cyber attack conducted **over the phone**. In vishing scams, attackers impersonate family members, representatives from well-known organizations (hospitals, banks or government agencies) to gain their victim's trust. They use social engineering tactics, preying on emotions like fear or urgency, to trick individuals into divulging confidential information or performing certain actions.

How Vishing Works:

- Cyber criminals place calls to potential victims, using a friendly or authoritative tone to gain their confidence.
- The callers may claim suspicious activity on one of the victim's accounts (bank, Amazon, etc.) or subscriptions, or offer a lucrative deal, persuading them to reveal sensitive data, disclose personal health information, or carry out financial transactions.
- In some cases, vishing scammers may manipulate caller ID information to appear more legitimate.

### Protect Yourself Against Phishing, Smishing, and Vishing:

1. **Be skeptical:** Always question unexpected messages or calls asking for personal information or immediate action.
2. **Verify the sender:** Double check the authenticity of emails, texts, or callers by contacting the organization directly through official channels.
3. **Use multi-factor authentication:** Enable two-factor authentication wherever possible to add an extra layer of security to your accounts.
4. **Educate yourself:** Don't become a victim of phishing, smishing or vishing. Stay informed about the latest cyber threats and best practices for online safety as it relates to the health-care sector. Take OntarioMD's Privacy & Security Training for the Health Care Sector. It's online, free and takes you through scenarios that have actually happened to clinicians.
5. **Install security software:** Use reputable anti-virus and anti-malware software to protect your devices from potential threats. Physicians can ask their OntarioMD Advisor for some suggestions.

As our digital world expands, so do the threats lurking in cyber space. Phishing, smishing, and vishing attacks prey on human vulnerabilities, using deception and psychological manipulation to steal sensitive information and cause financial harm to individuals or their practices. Awareness and vigilance are our best defence against these cyber threats. By staying informed, taking appropriate training, being cautious, and adopting robust security measures, we can safeguard ourselves and our data from falling victim to the cunning tactics of cyber criminals. Remember, your cyber safety is in your hands, and with knowledge and diligence, you can navigate the digital landscape with confidence.

If you would like more information on privacy and security training, resources you can download, need advice or have a question, OntarioMD is your trusted advisor on privacy and security for the health-care sector.

**Contact us at support@ontariomd.com.**