

# **ALARM - A 5-Step Plan Towards Better Security**

*By Neal O'Farrell*

The acronym ALARM represents the five most important steps every consumer and small business owner needs to follow if they want a foolproof way to minimize their exposure to cybercrime and identity theft.

ALARM stands for:

**A**ccept

**L**earn

**A**ssess

**R**espond

**M**aintain

And while it might also sound like a 5-step program towards recovering from substance abuse, there are many parallels. ALARM is a path to recovering from the apathy and indifference that makes most of us so vulnerable to these crimes.

It involves understanding why you could be a victim, how your attitude and behavior can make you vulnerable, how others (especially identity thieves) see you, and how you need to change that vulnerable behavior.

## **Step 1: Accept**

The first and most important step in any security plan is a full acceptance that the threats exist.

That means an acceptance of:

The seriousness and variety of the risks.

The likelihood that you will be a victim.

The likely long-term impact and cost if you are a victim

The need to take personal responsibility.

The need to take planned action now.

If you don't fully and truly accept that there are life-changing cyber threats out there, and that you're the only one who can really make a difference, then any further action is meaningless.

But if you do "accept," you're now ready to move on to Step 2 – Learn.

## **Step 2: Learn**

I once heard a senior executive at a well-known security firm tell a reporter that user education and awareness are an obstacle to security, and that users should instead leave security to technology. She was obviously just trying to sell more technology, but she couldn't have been more wrong.

When it comes to fighting cybercrime and identity theft a little knowledge is not a dangerous thing, and as part of the planning process you should take the time to learn as much as you can about:

What the threats and risks are.

Who the bad guys are.

What they want from you.

How they attempt to get it.

What exploitable mistakes they expect you to make.

What you can do to minimize your exposure.

What role security technology can play.

How that technology works.

## **Step 3: Assess**

Step 3 is where you really get to see yourself as the bad guys see you, and in this step your focus is on assessing and measuring your own vulnerability.

There are more than a dozen aspects of our daily lives that make us all vulnerable to cybercrime and especially identity theft, from the way we use computers and the internet, to the way we monitor our credit, handle our mail, and pay our bills.

Your next job is to assess where and to what extent you are vulnerable in areas such as:

Your attitude and behavior.

Your awareness and vigilance.

Your use of computers and the internet.

Your family security rules and expectations.

Use of credit cards.

How you handle your mail.

How you bank and pay bills.

How you monitor your credit.

How you create and use passwords.

How you manage your financial records.

How you behave in public.

The goal is to see yourself as the bad guys see you, but before they do. You have to first find your own vulnerabilities before you can proceed to the next and most important step – Respond.

#### **Step 4: Respond**

How you respond to everything you've learned will ultimately determine how well you're insulated from crime and that's why Step 4 is so important.

This step focuses on what security measures you're going to put in place to patch your vulnerabilities, and these "patches" could include:

Changes in your behavior, habits, and attitude.

Creating of a set of security rules for you and your family.

Better use of security technologies.

Changes in how you monitor your credit.

Changes in how you handle your mail.

Changes in how you run your business.

Changes in how you use and manage your credit cards.

Security around your home.

What you plan to do if you do fall victim.

The ultimate goal of Step 4 is to create a list of personal and family security rules that address the vulnerabilities you discover and which you can learn to live with.

#### **Step 5: Maintain**

The final step in planning your security is probably the easiest, but only if you've completed Steps 1 through 4. That's because if you've genuinely embraced all the other steps, Step 5 simply requires you to give yourself a regular checkup, to make sure that changes in your life have not created new vulnerabilities, and that you're up to speed on the latest threats, tricks and techniques used by the bad guys.

Good security is not a set-and-forget program, but requires you to regularly review and update your security so it addresses changes in the threat environment and in your lifestyle.

