For Sale – Your Data on the Dark Markets

By Lisa Traina, Partner, Traina & Associates

Here are three words that conjure an instant reaction of curiosity, trepidation or fear in most people: The Dark Web. The "dark web" refers to Internet content that physically exists on a series of encrypted networks that require special software configurations to access. The dark web is a sub-section of the "deep web," a part of the Internet that is not indexed by search engines.

The dark web was founded on the principle of an anonymous network created to help corporate whistleblowers, political dissidents, and government-controlled journalists communicate freely; in essence, to be a safe environment for communication without the fear of dictator governments knowing. Although some would say that is still true, unfortunately it isn't the main function of the dark web today. As with anything built with a positive purpose, there are those who seek to destroy it for their own gain through illegal ventures.

The dark web ecosystem has been flourishing since the early 1990s. Financial gain is the motivating factor for the many services advertised, and there are a number of threats for nonprofit organizations.

Data for Sale

Stolen email addresses, passwords, personally identifiable information (PII), bank account information, and other data are for sale on the dark web. A recent report by the Digital Citizens Alliance (DCA), for example, noted millions of email accounts and passwords associated with students, faculty, staff, and alumni at top higher education institutions available on the dark web.

The stolen credentials can be used in phishing emails that look like they are from a trusted sender such as your bank or a member of your leadership team. This can expose your nonprofit's network to malware if the recipient clicks a link or attachment. Other phishing schemes trick employees into wiring funds to a cybercriminal because they think the request is originating with a member of the leadership team.

And because many people use the same password on multiple sites, stolen credentials can be used to gain access to other cloud-based systems and online bank accounts.

Your Credit Card Number

Another service advertised on the dark web is "carding," the trafficking of stolen debit and credit card information. "Carders" are individuals who use stolen card information to make illegal purchases.

A typical week of using a corporate debit or credit card at a nonprofit might involve purchases of office and ministry supplies, gas, meals during travel, and other necessities. Every swipe at a terminal, every hand off to a store employee, and every online payment uses your card number. Criminals have highly organized enterprises in every state and country with the technical expertise to take those highly sought-after card numbers and make a profit faster than you can call your bank and report it.

Criminals have highly organized enterprises in every state and country.

Devices called ATM skimmers or POS (point of sale) skimmers — fake card readers made to look genuine — are often used to steal card numbers. Criminals are notorious for using skimmers at gas pumps by placing identical plastic parts over the original card reader. When you swipe your card, the fake reader stores your PIN and card number for later retrieval by the criminal who installed it.

For just a few hundred dollars, anyone can become a carder and sell your data. The physical hand-off of your card to a complete stranger who swipes and returns the card to you could theoretically involve a carder at any time or any place. A quick Google search will reveal hundreds of detailed tutorials on what it takes to be a professional carder. This is not a specialized enterprise just for cybercriminal gangs.

From Stolen Numbers to the Dark Web

The ease of becoming a professional carder makes the next step in carding simple. Once your nonprofit's credit card numbers have been captured, the carder sells them to buyers on carding markets that advertise on the dark web. Most carders will amass hundreds of numbers and sell them as "dumps" on the market of their choice. The markets often selected are eBay-styled in theme and function. Some sellers and buyers of cards even have a rating system in place, because there is fraud within fraud and carders will scam other carders.

Once a transaction is made, the buyer takes the "dumps" of the numbers and uses a $150 card writer to encode the information on blank cards. Each card is associated with the PIN number, and now can be used at ATMs to withdraw cash from your account.

An alternative and somewhat safer way carders use your card is for online shopping. Most e-commerce sites don't require a PIN code with purchases. Although there are safety measures in place when purchasing online, carders know which sites have few security checks that would raise red flags. The criminals then sell the products online at places like Craigslist, eBay, and auction houses, turning the merchandise into cash.

Corporate credit cards are used at many nonprofits. If your credit card is lost or stolen or you notice fraudulent charges on your bill, in most cases your bank or financial institution will refund the money lost and issue a new card. This safety net offers some peace of mind. Debit cards do not offer the same protections, so if you are not doing so already, you may wish to move away from frequent debit card usage.

Provide ongoing cybersecurity training to help all employees, volunteers, and board members understand the latest cybersecurity threats. This training should include topics such as phishing, strong passwords, and why the same password shouldn't be used on multiple sites.

Additionally, educate employees with a corporate credit card on the risks of stolen numbers. Train them to be wary of using ATMs in unfamiliar or low-traffic areas and to check gas pump readers to see if they are loose before swiping or inserting a card.

Review your nonprofit's bank account and credit card transactions very frequently, even daily, for fraudulent activity. Watch for small transactions in $1 to $5 increments that might indicate criminals testing validity before buying dumps. Many banks and card companies also offer text messaging notices of transactions, which can help you identify fraud instantaneously.

New cybersecurity threats arise at a breathtaking pace. Meanwhile, the underground continues to grow technically and financially, and every day a new carding forum arrives as soon as another is taken down by law enforcement. Being aware of what the dark web entails and taking few simple steps can help your nonprofit stay safe.

About the Author

Lisa Traina, Partner
Traina & Associates, a CapinCrouse Company
ltraina@capincrouse.com
o 225.308.1825

Lisa uses her more than 30 years of experience to assist organizations in implementing measures to secure data and manage risks efficiently and effectively. She is a nationally recognized speaker and author, and serves on the AICPA Cybersecurity Task Force. Lisa founded Traina & Associates in 1999 to provide IS security services to a broad range of industries. Traina & Associates joined CapinCrouse in January 2017.

About Traina & Associates*

Traina & Associates, a CapinCrouse company, has been providing information security services, including cybersecurity assessments, consulting, and training services, to financial institutions, nonprofit organizations, medical entities, professional services firms, and other organizations since 1999. Each year the firm performs hundreds of assessment, consulting, and speaking engagements with a team of experienced professionals retaining numerous certifications, including CPA, CISSP, CISM, CISA, CITP, CGMA, and CTGA. Each engagement is tailored to fit the unique needs of the organization, and information and reports are presented in a clear, concise manner intended for an audience with varying information systems (IS) knowledge. More information is available at trainacpa.com.

*Traina & Associates is an authorized trade name of Capin Technology LLC, a subsidiary of Capin Crouse LLP.

About CapinCrouse

As a national full-service CPA and consulting firm devoted to serving nonprofit organizations, CapinCrouse provides professional solutions to organizations whose outcomes are measured in lives changed. Since 1972, the firm has served domestic and international outreach organizations, universities and seminaries, foundations, media ministries, rescue missions, relief and development organizations, churches and denominations, and many others by providing support in the key areas of financial integrity and security. With a network of offices across the nation, CapinCrouse has the resources of a large firm and the personal touch of a local firm. Learn more at capincrouse.com.

CapinCrouse is an independent member of the BDO Alliance USA.