DEPARTMENT OF INFORMATION TECHNOLOGY **Monthly Report**

Cindy Knox, Information Technology Director
(978) 772-8220 ext. 123

Town of Ayer, Massachusetts
1 Main Street – Ayer, MA 01432

REPORT FROM INFORMATION TECHNOLOGY – DECEMBER 2022

PROJECTS / HARDWARE / SOFTWARE:

- Troubleshoot & resolve issues at Town Hall, DPW, Ayer Fire, and Council on Aging.
- Employee Security Awareness Training.
- Setup new employees: remove access for terminated employees.
- Set up new and replacement computers, phones, tablets, and printers.
- Dispose of old equipment.
- Facilitated 5 Zoom Meetings.
- Prepared FY24 IT Budget

WEBSITE / SOCIAL MEDIA:

- Maintain website and social media
- Monitor Daily
- Add video to the Town’s website and social media.
- Minutes, agendas, calendar, and page updates
- Post Notices to Announcements on the Website, Facebook, Twitter, and APAC as needed
- Post updates to the internal and external signage
- Promote local events.

STATISTICS:

Social Media / email:

1. Facebook page reach: 9.2K
2. Twitter followers: 1,490
3. Email subscribers: 4,500

WEBSITE:

1. Top Five Web Pages
    1. Online Payments
    2. Assessor
    3. Police
    4. Transfer Station
    5. Santa Parade

2. Number of page views: 25,612
3. Average visit duration: 2 min 20 sec

<u>One Out of 10 Threats Still Make It All the Way to the Endpoint</u>

I am happy to report that the Town’s end users actively seek out these threats and we have not seen any evidence of malware infecting any of the Town’s Systems in several years.

Despite good intentions, layered security measures, and efficacy claims by security solution vendors, new data shows that **email-based threats are still getting all the way to the Inbox**.

Given all that your organization has in place to stop threats from entering into your environment, you'd like to think it all gets stopped. Your security vendors certainly tell you that their solution stops some very high percentage of attacks – likely in the 99-point-something range. And the layered defense you've implemented is designed to address attacks from a number of directions, giving you a heightened chance of stopping an attack before it does any damage.

But new data from Acronis in their End-of-Year Cyberthreats Report shows that **11.7% of all attacks still make it to the endpoint**. This is nearly 11% increase from the previous quarter – meaning threat actors are getting better at avoiding detection and obfuscating the malicious nature of their emails.

Part of this "success" may be due to the short lifespan of a given piece of malware – according to the report (emphasis is mine):

The average lifetime of malware samples in November 2022 was ***1.7 days, after which a threat would disappear and never be seen again****. In Q2 2022, this figure was at* ***2.3 days, showing that malware is even more short-lived today*** *as attackers use automation to create new and personalized malware with a frequency that overwhelms traditional signature-based detection.* ***Seventy-four percent of the samples observed were seen only once*** *across our customer base.*

With this newfound data, it should be obvious that you should expect that malicious emails are going to find their way past your security solutions, making it absolutely necessary for your users to play a part in organizational security by being vigilant when interacting with email and the web.