

Little Red
Riding Hood:
A
Cybersecurity
Tale



TRAVIS NICHOLS

DIRECTOR OF
INFORMATION SECURITY,

SHELTER INSURANCE



Speed of Change... this is my experience in the U.S. and is spreading quickly throughout the world.



2018

2020

2022

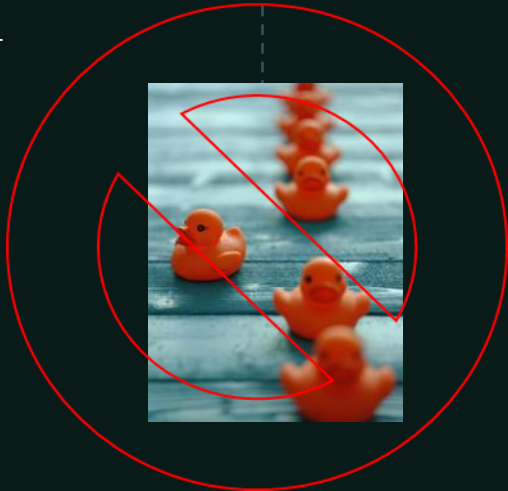
2016

2019

2021



Securityintelligence.com





Life at Little Red Riding Hood's House...
and maybe at your company or home.

Her Passwords

Multifactor Authentication!?

Phishing, Smishing, Vishing

Letter from Grandma

In 2015, the average user had 150 online accounts...



...today, she typically has 300.

blog.dashlane.com/world-password-day/





Her Passwords

- Little Red Riding Hood often reuses the same password with a slight twist like an exclamation mark, the season of the year, or a number.
- She tries not to think about what would happen if her browser crashed (along with the autofill). Since she has not had to type in some of her passwords for some time, she has quite forgotten them.
- Maybe it wouldn't be too bad... she does have some of her passwords on sticky notes around here somewhere, even a few stuck to the computer.



Multifactor Authentication!?

- “Yeah, I use multifactor authentication... sometimes.”
- I had to set up some security questions for a couple of accounts... and I’ll never forget my first dog’s name. I’ve posted dozens of pictures of her on Instagram.
- At work, they make me have something on my phone that I must click when I want to log on remotely. Sometimes it goes off at a weird time, so I just click OK.






Phishing, Smishing, and Vishing

- Phishing (email)
 - Malicious web links
 - Malicious attachments
 - Fraudulent data-entry forms
- Smishing (SMS / text)
 - Confirm before going to buy those gift cards.
 - Apple and Amazon tell you on their web site that they will not ask you for sensitive information via phone or text.
- Vishing (Voice)
 - Microsoft is not going to discover a virus on your computer and call you to help fix it.

From: Bank of America <crvdqi@comcast.net>
Subject: Notification Irregular Activity
Date: September 23, 2014 3:44:42 PM PDT
To: Undisclosed recipients: ;
Reply-To: crvdqi@comcast.net

Bank of America 

Online Banking Alert
Would be capitalized

Dear member:

We detected unusual activity on your Bank of America debit card on **09/22/2014**. For your protection, please verify this activity so you can continue making debit card transactions without interruption.

Please sign in to your account at <https://www.bankofamerica.com> to review and verify your account activity. After verifying your debit card transactions we will take the necessary steps to protect your account from fraud.

Grammatical Error

<http://bit.do/ghsdfhgds>

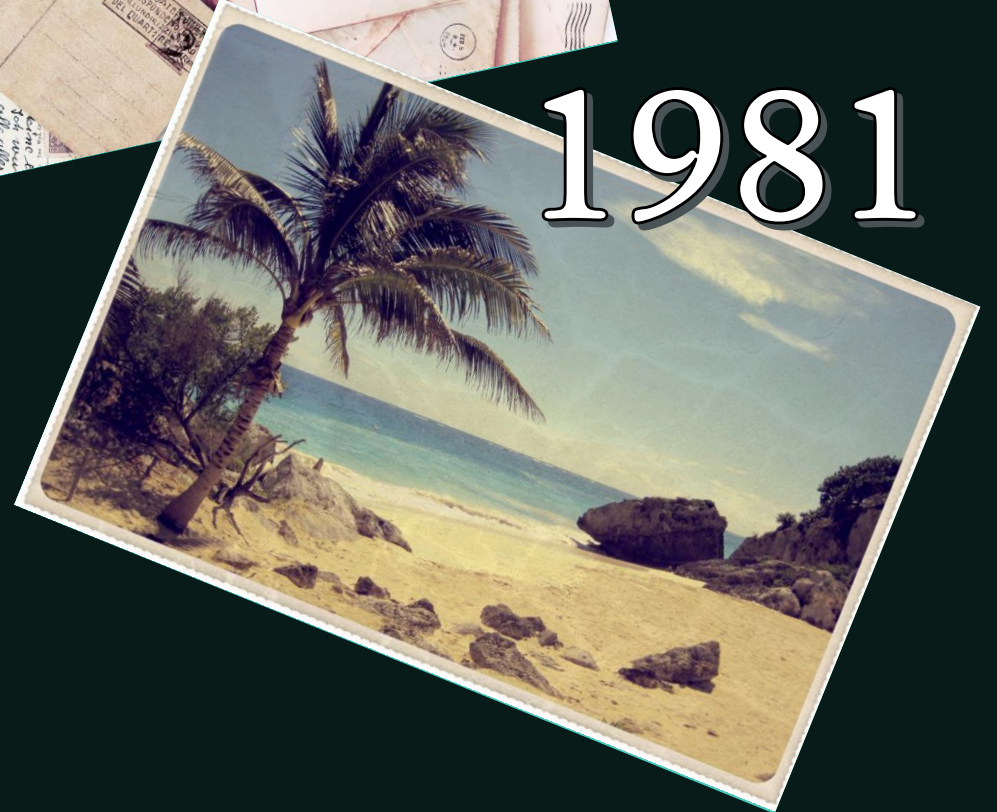
© 2014 Bank of America Corporation. All rights reserved.



Letter from Grandma

All in the header which you don't normally see.

- SPF (Sender Policy Framework)
 - Identifies who can send email as your domain
- DKIM (DomainKeys Identified Mail)
 - Verifies who sent the email and that it was not altered in transit
- DMARC (Really long)
 - DMARC policies tell your email server what to do with emails that do not pass SPF and DKIM verification





Into the Forest

Risk, not FUD

Everyone Needs to be on the
Security Team

Trust Your Instinct

Phishing Campaigns are Not Your
Enemy



Risk, not FUD

For years, enforcement of all types has used fear, uncertainty and doubt (FUD) to drive acquiescence.

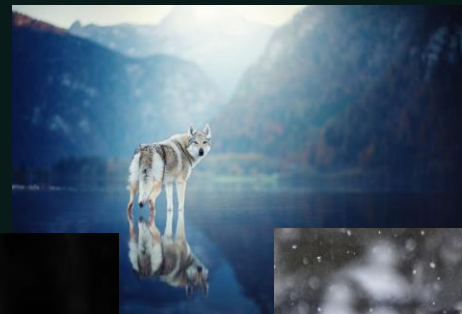
Business, especially insurance, is a calculated risk.





Everyone Needs to be on the Security Team

InfoSec cannot be everywhere... and it frustrates folks when we try to be. Part of being risk-driven is that Information Security communicates the risk in an understandable way, and everyone engages.





When all grows quiet, the forest warns: trust your instinct.

#1 Reason people give for falling for a phish – “I was going too fast.”





Phishing Campaigns are not Your Enemy

Imagine Little Red Riding Hood's little brother Fred dressing up to scare her in the forest - sometimes annoying, but harmless... just enough of a reminder to help her be aware of her surroundings.

- Shelter Insurance cut by ~73% the average number of times folks fell for training phishes by going to an at-least-once-per-month frequency for each employee. (September 2022)





Arrival at Grandma's House

Password Managers

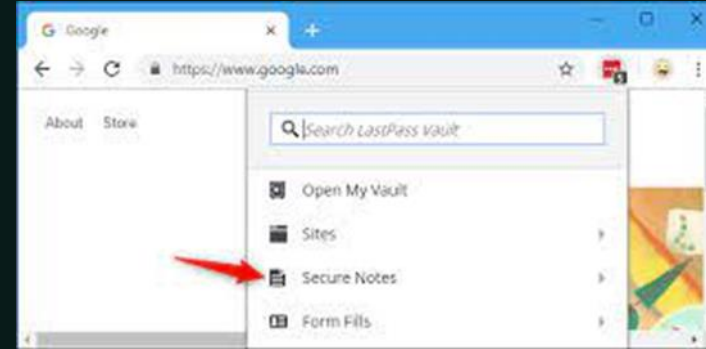
Minimal Marketplace

Expectations



Password Managers

- Can generate unique passwords/phrases.
- Can auto-fill the passwords (usually).
- Can share passwords *without* revealing the password.
- Basic (and useful) versions of password managers are at no cost.
- Can be run as an application or a browser extension on almost any device.



Minimal Marketplace Expectation for Cyber Controls

- Token Based Multi-factor Authentication (MFA)
- Vulnerability Scanning & Patch Management
- Endpoint Scanning & Response (EDR)
- Email Filtering & Security (SPF/DMARC/DKIM)
- Social Engineering Exercises & Awareness Training
- Identity, Access and Privileged Access Management
- Network Segmentation: Secure RDP, VPN, OT/IT
- Disaster Recovery Testing, BCP, & Backups
- Incident Response Plan (Written & Tested)

Used with 9/21/2022 permission
from Cody Olsen.