https://skvare.com

Why talk about privacy and security?

Why This Talk

- We care about our security and privacy.
- We care about other people’s security and privacy.
- State and federal governments care about security and privacy.
- The survival of our organizations depends on the proper care in handling private information.

Statistics

- More Than $3.5 Billion Was Lost to Cyber Crime Globally in 2019.
- BEC/EAC scams (more than $1.7 billion)
- Email Spoofing (more than $300 million)

https://securityboulevard.com/2020/05/the-definitive-cyber-security-statistics-guide-for-2020/

skvare
square and uneven

What is [digital] privacy

Privacy Is All About Personal Information

According to westlaw.com,

- Personal Information is data that can be used to identify, locate, or contact an individual, alone or when combined with other personal or identifying information.

What is [digital] security?

[Digital] Security Defined

"Security is using tools and best practices to keep private information, private."

– ME.

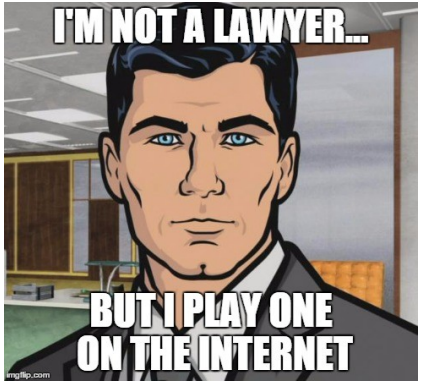
skvare
square and uneven

Importance and legalities…

Disclaimer...

“I am not a lawyer, and if you need one, I recommend you consult one.”

– also ME.



skvare
square and uneven

Legal Stuff

- GDPR - General Data Protection Regulation
- CCPA - California Consumer Privacy Act
- Most States require some form of "**reasonable security procedures and practices.**"

  https://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx

Case Study: Blackbaud

The Blackbaud 2019 Data Breach Affected 45,000 Nonprofits

skvare
square and uneven

skvare
square and uneven

..

The Fallout...

- 23 class action lawsuits are underway against Blackbaud...
- One commentator writes, **"How does a nonprofit come back from that?"**

  https://forpurposelaw.com/blackbaud-data-breach-fallout-nonprofits/

How was Blackbaud hacked?

Not Hacked by Traditional Means...

Traditional exploitation:

- Malicious website
- Malicious email attachment
- Malware, Worm, Trojan horse, Virus
- Out of date Operating system

NONE of the above

Deception

Blackbaud was hacked via:

- **Social Engineering**
- **Phishing**
- **Data Ransom**

Know your enemy: Social Engineering

Social Engineering

"(in the context of information security) The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes." - Oxford dictionary

skvare
square and uneven

Know your enemy: Phishing

Phishing

"Phishing is the fraudulent attempt to obtain sensitive information or data, such as usernames, passwords and credit card details or other sensitive details, by impersonating oneself as a trustworthy entity in a digital communication." - Wikipedia

skvare
square and uneven

There's issue with your American Express account

AE

American Express <administraciones@pentagon-seguridad.cl>
To hashedout@thesslstore.com

Reply | Reply All | Forward | ...

Fri 11/8/2019 5:29 AM

This message was sent with High importance.
If there are problems with how this message is displayed, click here to view it in a web browser.

AMERICAN EXPRESS

Review Your Information.

Due to recent activities on your account, we placed a temporary suspension untill you verify your account. You need to review your information with us now on 11/8/2019 10:28:38 AM.

To continue using our American Express Online service, we advise you to update the information about your account ownership.

Click here to review your account now

For the security of your account, we advise not to notify your account password to anyone. If you have problems updating your account, please visit American Express Support.

Sincerely,

Fwd Important: [App] - [services] We'll not provide our service due to invalid information Chase ID : #5848784506...

PL

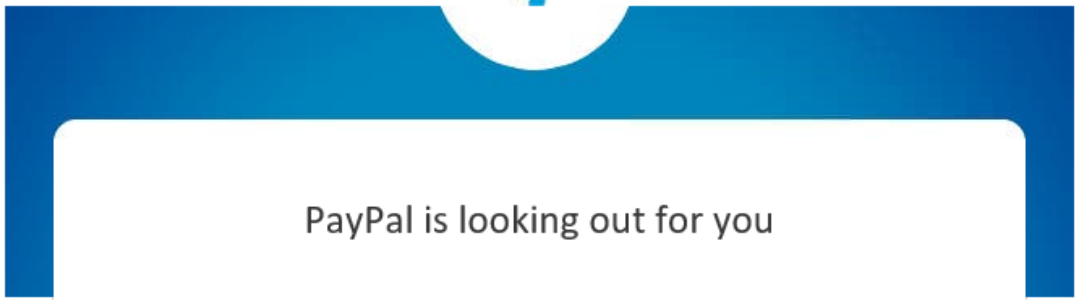
paypal letter <replynore@petersenfamilychiro.com>
To Adam Thompson - The SSL Store™

Reply | Reply All | Forward | ...

Wed 9/2/2020 5:18 PM

If there are problems with how this message is displayed, click here to view it in a web browser.

Bing Maps Action Items + Get more add-ins



PayPal is looking out for you

At PayPal, safety and security are our top priorities, and we routinely monitor accounts for any unusual activity. We've taken extra precaution to confirm that your PayPal account is secure and have assigned your account with a temporary limited.

You will need to restore your account to re-access your PayPal account.

To restore your account:

1. Click "Log In Now." In the below section.

Advanced Phishing Utilizes Social Engineering

According to Microsoft,

- Spear phishing uses focused, customized content that's specifically tailored to the targeted recipients (typically, after reconnaissance on the recipients by the attacker).
- Whaling is directed at executives or other high value targets within an organization for maximum effect.
- Business email compromise (BEC) uses forged trusted senders (financial officers, customers, trusted partners, etc.) to trick recipients into approving payments, transferring funds, or revealing customer data.

Email Spoofing

Warning: All Email headers can be forged.

The “From:” address can be perfectly spelled, and perfectly forged.

Know your enemy: Data Ransom

Data Ransom: Too Late, You Lose.

"Ransomware encrypts your data and demands payment to decrypt it almost always starts out in phishing messages." - Microsoft

- If it truly is a data ransom, it's probably too late. This is not something we want to go through.
- Keeping secure off-site backups data can help, but is not a guarantee.

5 Things we can do right now

1. Protect From Physical Theft

If my work cell or laptop are stolen, I do not want to put my organization at risk.

- Have a policy to Encrypt and auto-screen lock all local work computers and cell phones.

  https://spreadprivacy.com/how-to-encrypt-devices/

- Make regular off-site (online) backups, and consider encrypting the online backups depending on the nature of the data.

2. Implement Phishing Email Scanning

A few options,

- Premium business email providers who offer phishing scanning:

  Google G-suites
  Microsoft Office 365
  Amazon Workmail

- Many Website Hosting providers offer email plans that use **Rspamd** email scanning.

3. Implement DNS Filtering

Many common malware and phishing websites in the wild are blocked by IBM's **quad9** DNS service or Cloudflare's **1.1.1.1** DNS service.

Setup only takes a few minutes.

- MacOS / Windows 10 video tutorials are at https://www.quad9.net/ or https://1.1.1.1/

4. Password Managers

Use a password manager.

- Chrome and Firefox browsers have built-in password managers and strong password generators.

The password manager isn't going to offer to fill in the password on a fake website.

That's a major clue that you might have accidentally clicked on a phishing link.

5. 2-Factor Authentication

Pros:

- 2-factor Authentication ties your website login to your cell phone. In order to login, you will enter your password, and then you will be asked for a unique code that is on your cell phone.
- Does improve security

Cons:

- Can be thwarted by sophisticated phishing sites that use Modlishka https://github.com/drk1wi/Modlishka
- False sense of security
- Can be annoying to use

Summary

.

We fight for online privacy and security together

Send me an email! :)

Adam Schaefers
Devops, Skvare.com

Contact me:
adam@skvare.com

skvare
square and uneven

https://skvare.com