From: SCENE <newsletter@mail.scene.ca>
Subject: [SPAM] Important: You should update your password
Date: Wed, 01 Mar 2017 19:03:22 -0500

Reset now | Online Version

SCENE

RESET YOUR PASSWORD

TO ACCESS YOUR SCENE ACCOUNT

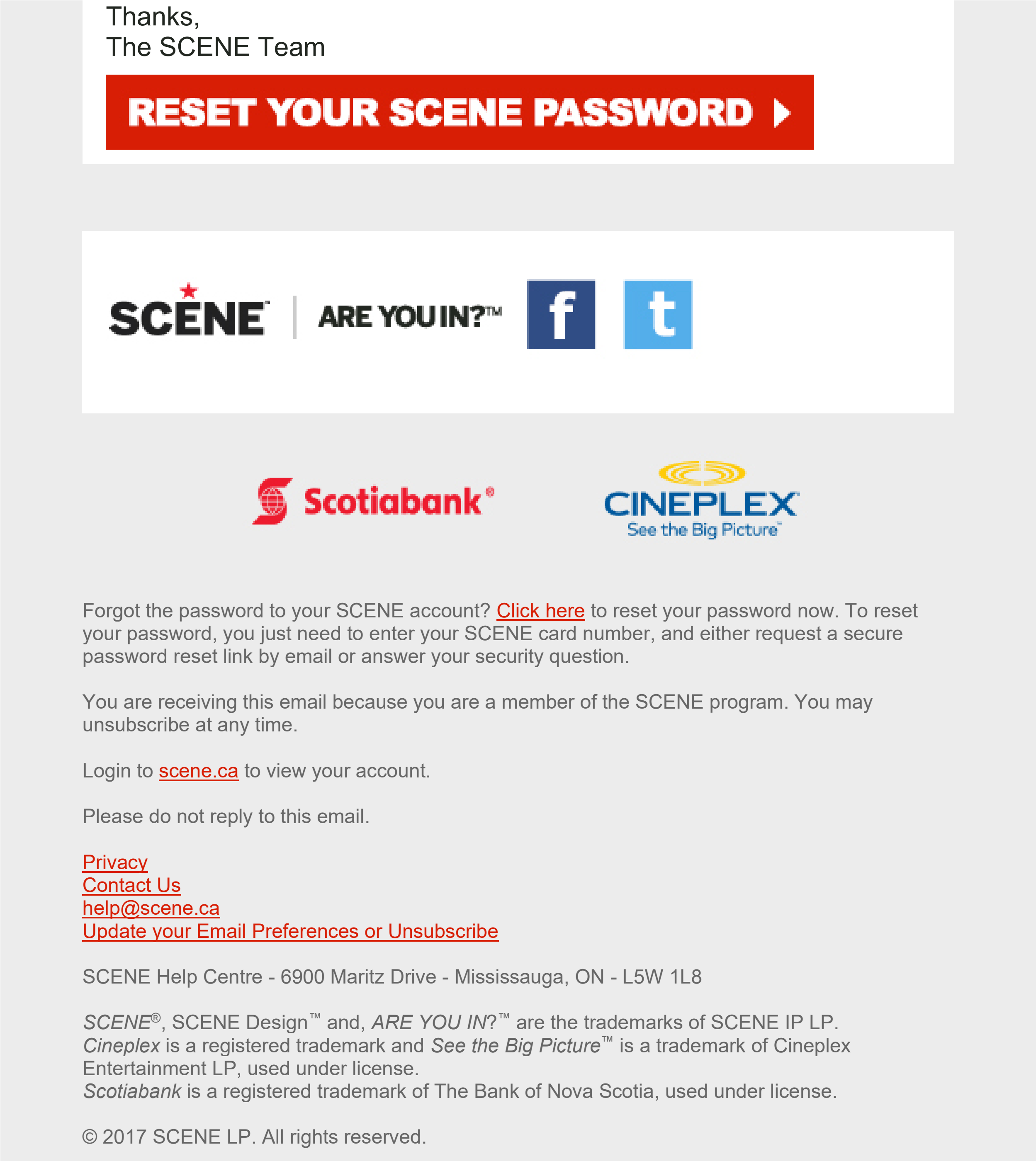
Dear SCENE Member:

As a valued SCENE member, we want to draw your attention to recent news about thefts of user information from a number of popular online services. As a result of these incidents, a large volume of private user information, such as email addresses and passwords, has been exposed.

Security experts agree that using the same username and password for multiple services is a risky behaviour. Whether your account is with a retailer, a bank, or lesser known website or mobile app, you could be unknowingly putting your personal information and identity at risk.

To ensure your security, we encourage you to reset your password and please ensure that it is unique, strong and private.

You can update your SCENE password by visiting scene.ca or clicking the link below and following the easy instructions.



Thanks,
The SCENE Team

Forgot the password to your SCENE account? Click here to reset your password now. To reset your password, you just need to enter your SCENE card number, and either request a secure password reset link by email or answer your security question.

You are receiving this email because you are a member of the SCENE program. You may unsubscribe at any time.

Login to scene.ca to view your account.

Please do not reply to this email.

Privacy
Contact Us
help@scene.ca
Update your Email Preferences or Unsubscribe

SCENE Help Centre - 6900 Maritz Drive - Mississauga, ON - L5W 1L8

SCENE®, SCENE Design™ and, *ARE YOU IN*?™ are the trademarks of SCENE IP LP.
Cineplex is a registered trademark and *See the Big Picture*™ is a trademark of Cineplex Entertainment LP, used under license.
Scotiabank is a registered trademark of The Bank of Nova Scotia, used under license.

Dear SCENE Team,

I have questions about changing my password as per your email of Wed, 01 Mar 2017.

- Why do I have to change my SCENE card password if your security was not breached? It is certainly wise to warn users not to reuse their passwords, but shouldn't that be the *only* reason a user needs to change their password at your site…unless, of course, your systems were breached like other “popular online services” but, like most online services, you don’t want to admit that. (Or, that you've never read OWASP or NIST about important things like security.)

- If “passwords were exposed”, they were stored in plain text instead of salted and hashed as done by adults in the ICT industry. Even hashing alone is known to security simpletons. Storing passwords in plain text is done by clueless script kiddies. You know, your guys.
- Why did you compose the email to appear like a very good phishing scam? e.g. “Click here to reset your password now. …you just need to enter your SCENE card number, and …answer your security question.”
- Have you fired the CIO/CSO/CISO who hired those `dunderheads`?
- To whom do I send my consulting invoice?

This is my current password which used to work: “vXChuG3Tv7!bg%Gwxtf@”. (It was *never* used on any other site because I'm not an idiot.) But when I try to sign on with the current password to change it, this message is issued: "This value should be alphanumeric." The *only* edit for a current password should be that its hash matches the one in your system (or does not match…just so you are clear on the other possibility). What ditz on your programming staff applied new password editing rules to existing, previously valid, passwords on the sign-in form?

With difficulty and much ICT professional consternation, I managed to convince your system to change my password. Your email told users “to reset your password and please ensure that it is unique, strong and private.” Your site's edit for pure alphanumeric characters, i.e. *only* Latin letters A-Z or Arabic digits 0-9, in the password makes the conventional concept of “strong” simply impossible.

Tell the `null` values (your staff masquerading as programmers) who never thought beyond their own hours, days, and possibly weeks of deep experience that:

- If the user can type a password, your system should accept all the bits in the byte.
    - In common usage, “alphanumeric” includes any character on an ordinary keyboard.
        - The strict definition of "alphanumeric" should not be a constraint in passwords.
        - That your staff even knew the strict definition of "alphanumeric" is incredible. (word used advisedly)
    - Any security expert—even the ones without the angstrom depth of insight your staff have demonstrated, in the aggregate no doubt, and even dorks who don't know any better—will advise that "strong" passwords include other symbols in addition to pure alphanumeric Latin letters & Arabic digits. The real experts will know that the only strong password is a long passphrase.

- Entering a new password longer than 30 characters results in the message ”`This value seems to be invalid.`”
    - In what way? You seem unsure. Would you mind revealing the mystery of that tentative conclusion?
    - Does this mean your user account system uses an out-of-date hashing function incapable of storing long passwords?
- Current passwords are *never, ever* edited on the sign-in form, then rejected *before* checking in the user profile database. (This was indicated earlier but you've probably forgotten it by now.)
    - A database is a place where there is something called information…ask a grown up.
- Your password change procedure accepted a new password of 30 characters.
    - Your sign on screen edits the password (remember, it should not) and rejects it with this message:
      `"The length of the Password must be between 0 and 20 characters."`
    - This is an edit (read a textbook) that belongs on the password *change* screen, not on the sign on screen (remember, no pre-editing there).
    - So, after your system accepted a new 30-character password, it will not let me use it. Pity, because long length *is* strength. IT professionals, the ones *not* on your staff, know this.
    - Sadly, the 20 character limit is likely correct because it strongly indicates that the hashing routines you recently implemented are out of date. Cancelled and superseded. Wrongly used by people who are wrong. And two wrongs don't make a right.

Please sack the dolt who edits a current password. And the dullard who thinks only pure alphanumerics should be allowed. And the doofus who thinks the minimum length of a password can be zero. And the dimwit who told the dunderhead that the maximum length was 20 and the other doofus that it was 30.

This sort of incompetence was a joke in the 1980s. Has everyone with any sense retired before passing on tacit knowledge to people who would listen?

We are not done yet.

Hire someone who took an introduction to programming course and learned how to deal with spaces in a postal code, i.e. strip them all out before checking for a match with the address. The space is NOT part of a postal code − Canada Post will tell you this, they know. Really. – a space is part of the “output edit mask”. Look up that phrase up in a textbook (something written by people who know WTF they are doing).

Of course, if you do fire those on your staff whose incompetence is described herein, you might no longer have many staff but that would be a good start.