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

RESET YOUR SCENE PASSWORD ▶

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.
- If "passwords were exposed", they must have been stored in plain text instead of salted and hashed as is the ICT industry's best practice.

- Why did you compose the email to appear like a very good phishing scam?
  e.g. "<u>Click here</u> 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 who didn't do their due diligence?
- 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 in order to change it, this message is issued: "This value should be alphanumeric." The *only* edit for a current password should be that it matches the one in the system (or does not match...just so you are clear on the other possibility). What idiot on your programming staff applied new password editing rules to existing, previously valid, passwords?

With difficulty and much ICT professional consternation, I managed to convince your system to change my password.

Tell the `null` values (your programmers) who never took any of my classes or thought beyond their own weeks and months of deep experience that:
- The strict definition of "alphanumeric", i.e. Latin letters and Arabic digits, should not be a constraint in passwords.
  - Any security expert—even one without weeks or months of deep experience—will advise that strong passwords must include other symbols in addition to pure alphanumerics.
  - In common usage, "alphanumeric" includes any character on an ordinary keyboard.
  - Your email told users "to reset your password and please ensure that it is unique, strong and private." The edit for pure alphanumeric makes the conventional concept of "strong" simply impossible.
- 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 conclusion?
- Current passwords are *never* pre-edited on the input screen and rejected before checking in the database. (I indicated that 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.

- o Your sign on screen pre-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."`
- o 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).
- o So, after your system accepted a new 30 character password, it will not let me use it. Pity, because long length *is* strength.

Please sack the idiot who pre-edits a current password. And the one who thinks only pure alphanumerics should be allowed. And the one who thinks the minimum length of a password can be zero. And the idiot who told one programmer the maximum length was 20 and another 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're not done yet.

Hire someone who took my 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. The space is NOT part of the code (Canada Post will tell you this), it 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).

There must be a less redundant word than idiot for the IT staff responsible; try any of these: `fool, ass, halfwit, dunce, dolt, ignoramus, cretin, moron, imbecile, simpleton informaldope, ninny, nincompoop, chump, dimwit, dumbo, dummy, dum-dum, loon, dork, sap, jackass, blockhead, jughead, bonehead, knucklehead, fathead, butthead, numbskull, numbnuts, dumb-ass, doofus, clod, dunderhead, ditz, lummox, knuckle-dragger, dipstick, thickhead, meathead, meatball, wooden-head, airhead, pinhead, lamer, lamebrain, peabrain, birdbrain, mouth-breather, scissorbill, jerk, nerd, donkey, nitwit, twit, boob, twerp, hoser, schmuck, bozo, turkey, chowderhead, dingbat, mook.` Of course, if you do fire those on your staff who match these words, you might not have many staff left but that would be a good start.