expel

CYBERSECURITY AWARENESS MONTH

Cybersecurity Awareness Month 2022 **Tips & Tricks**

This Cybersecurity Awareness Month, the National Cybersecurity Alliance is promoting four key security behaviors to encourage individuals to take control of their online lives.

To support these behaviors, we're providing some guidance to help you improve your own cybersecurity posture, too!

1. **Always enable multi-factor authentication (MFA), but also have a back-up plan.**
   - It can feel daunting to think about all the various hundreds (pray tell thousands?) of applications you use...some daily and some hardly ever. Work on coming up with a list of the applications you use that have sensitive information or would have a broad impact if compromised (hello bank accounts and social media!). Have you enabled MFA there? If not, go ahead and do it now. Don't wait.
   - Once you've got MFA enabled, don't assume it's foolproof. Sometimes hackers will use brute force to bypass MFA by repeatedly sending push notifications to authorize a login. If you start getting a bunch of notifications requesting approval to login, just ignore them and don't be tempted to approve it to get the notifications to stop.

2. **Don't rely on your memory or sticky notes to keep track of all your passwords.**
   - Save time logging in anywhere by skipping the username and password prompt. Install a password manager. It'll generate safe passwords for you, log you in with one click, and keep your account much safer.
   - When your favorite website tells you they lost your password to hackers, you can change just one password instead of a dozen (or more) because password managers help you use a unique password on every website (that you don't even have to memorize).

3. **Stop ignoring that "software updates available" notification.**
   - While it's easy to put off software updates for another day, you could be leaving yourself susceptible to security vulnerabilities.
   - A lot of operating systems and app stores update automatically. If you have a choice, opt-in for these automatic updates. But if you need to update manually, use a natural break in the day—grab coffee or lunch and get it done.

4. Avoid taking the bait on a costly phishing scam.

- Email subject lines can give you a heads up that something's phishy. These were the top subject lines in malicious emails submitted to the Expel SOC in Q2 2022:

Top subject lines
Blank subject
Fax Delivery Report
Order Confirmation
Business Proposal Request
Request
INQUIRY
Meeting
'=Office365Alert@Microsoft.com=
Review financial document

- Hackers tend to target people based on their role and often go after those who receive a lot of external emails. For example, finance teams may come across financial-themed campaigns with popular subject lines, such as "URGENT:INVOICES," while recruiters may see resumé-themed phishing lures.
- If you suspect the email might be a phishing attempt, look at the email sender. These emails will sometimes look like they're coming from a real company, but the company name might be misspelled by one letter, or a zero might be used rather than an O, for example. Hover your mouse over any links to see where they'll bring you (but don't click!). And never open an attachment in a suspicious email. If you're still not sure, contact the person who sent you the message through another channel, and ask them about it. Just be sure not to "reply" to the email.
- If you get a phishing email, report it to your company's security team through its phishing process.