TWO-FACTOR AUTHENTICATION

WHEN MOST OF US HEAR THESE WORDS, WE REACT WITH ANYTHING FROM A YAWN TO AN EYE ROLL TO A VISCERAL REACTION OF “NO, THAT’S NOT FOR ME.”

However, putting this extra layer of protection between cyber attackers and your sensitive data can make all the difference.

If you have ever attended a security awareness session, you have heard how important it is to have strong passwords. The problem is that passwords can be compromised. For example, people respond to phishing emails or enter log-in information on webpages that resemble the log-in page for their bank, and POOF! The hacker has the information needed to reroute paychecks, move funds, and steal identities.

Two-factor authentication is a solution that is being adopted everywhere, from Facebook and Google to banks, credit card and cell phone companies, and the University of Arizona.

In this issue, you will learn what two-factor authentication is, why it is a good habit to adopt, and how easy it is to use here at UA.

WHAT IS TWO-FACTOR AUTHENTICATION?

SOMETHING YOU KNOW + SOMETHING YOU HAVE

Two-factor authentication puts an extra layer of security on your accounts by requiring you to have something you know (e.g., bank account username and password) and something you have (e.g., cell phone receiving text messages with additional code verifying your account).
**WHY DO I NEED IT?**

Quite simply, passwords are no longer enough protection, especially for sensitive information, such as your bank accounts, tax and payroll documents, and other information criminals might find attractive.

Many passwords are too weak, either because they are short or because they don’t include enough variables (upper/lower case letters, numbers and special characters).

And, even if you have a strong password, it could be stolen, guessed, hacked, or unsuspectingly revealed to someone with malicious intent.

Also, we have so many to remember, that we take the occasional shortcut and reuse passwords, even in places where we should be using unique ones, and these shortcuts increase the chances of your accounts being compromised.

However, by having two-factor authentication in place, only someone who knows your password and also has another item (e.g., your cell phone or smart phone, tablet, or landline) will be able to log in to your account.

**WHERE SHOULD I USE IT?**

You should definitely consider using two-factor authentication for your most sensitive data and accounts, especially on banking and credit card websites.

If two-factor authentication is available for an account, use it. Over time, it will be second nature to do so.

**CULTURE CHANGE: MAKING SECURITY A HABIT**

Back in the old days (aka, the 1980s), mandatory seatbelt laws began to be enacted. At first, many people complained that they were uncomfortable or too much of a bother. Eventually, people became so used to them that now it feels unnatural to not wear one. And it was a good habit to develop – seatbelts save lives...

Two-factor authentication becomes a habit over time as well, and since it can protect your financial information, identity and privacy, it is worthwhile to adopt.
**WHAT IS NETID+?**

NetID+ is the UA’s two-factor authentication resource. When applications and services require NetID+, it can prevent anyone but you from accessing using your credentials, even if an attacker knows your password.

After you sign up for NetID+, you will complete the first authentication step by entering your UA NetID and password on the UA WebAuth page, as you normally do. You can complete the second step in a variety of ways, depending on your preferences and the methods available to you. These methods include:

- verifying through phone calls entering one-time use passcodes received through text messages
- generating one-time use passcodes via the Duo Mobile app
- responding to an alert on your smartphone or tablet
- entering a bypass code, which can be generated after enrollment

Click [here](#) to enroll in NetID+.

---

**FOR MAXIMUM SECURITY, GO GLOBAL!**

Currently, only certain websites require the use of NetID+. However, you can increase your protection by enabling Global NetID+. By opting in to this feature, all of your WebAuth logins will require NetID+, ensuring only you can log in with your credentials.

**WHAT CAN GLOBAL NETID+ PREVENT? CONSIDER THE FOLLOWING SCENARIO:**

On February 26, 2014, UA faculty and staff received an email that appeared to be sent from a UA department, complete with a UA logo at the top. Recipients were warned that their webmail had been blocked for security reasons, and directed them to log into the “SecureMail Center.”
When recipients clicked on the link, they were led to a spoofed UAConnect page. Users unwittingly entered their NetIDs and passwords, and hit “sign in.” At this point, their credentials were sent to the attacker, and they were redirected to the real UAConnect page. For a full illustration, click here.

*The extra few seconds it takes to use Global NetID+ can help protect you from this scenario becoming your reality.*

**SET UP YOUR LIFELINES!**

There may be a time when your preferred device is unavailable. For this reason, it is a good idea to set up at least one Lifeline. This could be a landline (such as your work or home phone) or a line belonging to someone you trust, and with whom you have fairly consistent contact should the need arise.

**PRINT BYPASS CODES**

Bypass codes are one-time use passcodes you can print and keep in a secure location (such as your wallet) for a time when you may not have access to your cell phone and landlines.

**But Remember . . . You Still Need to Protect Your Passwords!**

Two-Factor authentication is an extremely effective extra layer of protection. However, remember there are still applications and systems where NetID+ is not in use, so it is still critical to protect your passwords, especially your NetID password. Keep “SOMETHING YOU KNOW” as “SOMETHING **ONLY** YOU KNOW.”

**NETID+ RESOURCES**

- [NetID+ FAQs](#)
- [NetID+ Tutorials](#)

---

**SECURITY TIP:**

*There is a website that compiles lists of companies and websites that offer two-factor authentication.*

Go to [Two Factor Auth (2FA)](#) to check.

---

**SecureCat Courier is distributed by Information Security Liaisons for UA Information Security.**

[UA InfoSec Web Site](#) | [Contact Us](#)

UA INFORMATION SECURITY
1077 N. Highland Avenue
Tucson, Arizona 85721
520.621.UISO (8476)

©2014 Arizona Board of Regents